FEDERAL NETWORK MANAGEMENT MARKET

1991 - 1996

INPUT

About INPUT

INPUT provides planning information, analysis, and recommendations for the information technology industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions.

Subscription services, proprietary research/consulting, merger/acquisition assistance, and multiclient studies are provided to users and vendors of information systems and services. INPUT specializes in the software and services industry which includes software products, systems operations, processing services, network services, systems integration, professional services, turnkey systems, and customer services. Particular areas of expertise include CASE analysis, information systems planning, and outsourcing.

Many of INPUT's professional staff members have more than 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed as a privately held corporation in 1974, INPUT has become a leading international research and consulting firm. Clients include more than 100 of the world's largest and most technically advanced companies.

INPUT OFFICES

North America

San Francisco
1280 Villa Street
Mountain View, CA 94041-1194
Tel. (415) 961-3300 Fax (415) 961-3966

New York
Atrium at Glenpointe
400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050 Fax (201) 801-0441

Washington, D.C.
INPUT, INC.
1953 Gallows Road, Suite 560
Vienna, VA 22182
Tel. (703) 847-6870 Fax (703) 847-6872

International

London
INPUT LTD.
Piccadilly House
33/37 Regent Street
London SW1Y 4NF, England
Tel. (071) 493-9335 Fax (071) 629-0179

Paris
INPUT SARL
24, avenue du Recteur Poincaré
75016 Paris, France
Tel. (33-1) 46 47 65 65 Fax (33-1) 46 47 69 50

Frankfurt
INPUT LTD.
Sudetenstrasse 9
D-6306 Langgöns-Niederkleen, Germany
Tel. (0) 6447-7229 Fax (0) 6447-7327

Tokyo
INPUT KK
Saida Building, 4-6
Kanda Sakuma-cho, Chiyoda-ku
Tokyo 101, Japan
Tel. (03) 3864-0531 Fax (03) 3864-4114

M&S 459/01 5/91

OCTOBER 1991

FEDERAL NETWORK MANAGEMENT MARKET

1991-1996

INPUT®

1953 Gallows Road, Suite 560 Vienna, VA 22182 (703) 847-6870

Published by
INPUT
1280 Villa Street
Mountain View, CA 94041-1194
U.S.A.

Federal Information Systems and Services Program (FISSP)

Federal Network Management Market, 1991-1996

FINWM • 301 • 1991

Abstract

INPUT expects the federal network management market to grow from $91 million in FY 91 to $180 million in FY 96, at a compound annual growth rate of 15%.

The professional services component of network management, while remaining the largest category, will lag the other categories (hardware and software) in growth rates. Most agencies intend to self-manage their networks, without using a contractor.

To date, federal departments have followed a path similar to that of the private sector in managing their networks. Netview and Novell are the most common wide-area and local-area network management products. Currently, one-quarter of federal departments contract for wide-area network management, while only one-tenth contract for local-area network management.

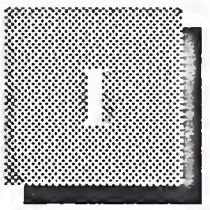
This report contains 106 pages and 36 exhibits.

Table of Contents

Table of Contents (Continued)

Exhibits

Exhibits (Continued)



Introduction

A Purpose and Scope

Managing networks has always been complex. With the increasing demand for integrated networks and systems, the complexity is not expected to decline. Networks are increasingly critical to successful operations and are continually impacted by changes in requirements and technology.

Complicating an already complex situation has been the rapid growth of local-area networking. Prior to the introduction of PCs and workstations, networking needs were limited to what are now referred to as wide-area networks.

Growth of local-area networking has given rise to significantly greater concerns about the flow and control of an organization's data. While circuit speeds have increased substantially over the past few years, the speed of wide-area networks is still limited when compared to local-area networks. Data delivered to a mainframe from a wide-area network is typically at speeds of 4.8-9.6 Kbps. Data delivered to a PC or a workstation over a local-area network may be at speeds in excess of 150 Mbps. Further complicating the situation has been the (apparent) lack of progress in finalizing equipment connectivity standards.

The lack of standards, proliferation of PCs and workstations, dramatic increases in circuit speed, and growing need for organizational connectivity have led many organizations to question the best way to connect and manage their networks. To some, FTS 2000 is an obvious answer, perhaps too obvious. Others are not at all certain that FTS 2000 will be able to successfully integrate local- and wide-area networks.

A key objective of the report is to examine the federal government market for network management. The report examines issues and trends driving and hindering growth of the market.

The report addresses a number of specific questions, including:

- How are wide-area networks typically managed today? Are they managed with in-house staff or through contracted services?
- How are local-area networks typically managed today?
- To what extent are local-area networks (LANs) connected to wide-area networks today? Will this need grow over the next five years?
- Is federal agency attention focused on establishing connections between the growing number of LANs or are LAN connections being made in the context of larger (enterprise) networks?

The key objectives of the research are to identify the current size of the market for network management products and services and to project the market size for the next five years.

B

Methodology

Research for this report included a review of published data to identify activities and trends that have been noted and primary research with government agencies. Key elements of the research included the following:

- A review of background data about trends and directions in network management
- A review of background data about key issues affecting the successful management of networks
- Interviews with large and small federal government agencies to determine primary methods of managing networks today
- Interviews with federal agencies to assess plans to develop integrated (local- and wide-area) and enterprise networks

To develop an understanding of agency perspective of needs and requirements, the interviews included both objective and subjective questions. The objective questions were oriented to developing an understanding of how (wide- and local-area) networks are connected today and whether they might be interconnected in the future. The subjective questions were oriented to developing an understanding of what agencies consider to be the best method of developing complex networks and their requirements for local-area network management systems.

C

Report Organization

Following the Introduction, the report is organized into three major parts.

- Chapter II is an Executive Overview of the report.
- Chapter III provides a forecast for the market for network management products and services.
- Chapter IV discusses the types of local- and wide-area networks and how agencies manage them today. Chapter IV includes a discussion of trends toward internetworking and enterprise-wide networking. Chapter IV also includes a number of conclusions and recommendations.

Executive Overview

A

Federal Market Pressures

The market for network management products and services is strongly influenced by pressures on the federal telecommunications market. Pressures that stimulate the growth of telecommunications stimulate the need for network management products and services. Pressures that inhibit growth of network use directly affect the need for network management.

Exhibit II-1 summarizes the major impacts on the federal telecommunications market. There is a direct relationship between these and the federal market for network management products and services.

EXHIBIT II-1

Major Federal Telecommunications Market Impacts

- Budget and deficit reduction
- Policy and regulation
- FTS 2000
- Interoperability
- EDI/E-Mail
- Technological advances
- Vendor competition

Pressures to reduce the federal budget and deficit is creating both positive and negative pressure on spending for telecommunications and network management products and services.

- On the negative side, departments are receiving increased pressure to reduce spending, particularly spending that will increase operating costs. This pressure significantly influences a department's decision process, generally reducing spending levels for new products and services. Many decide to continue 'muddling along' for a while longer with products already implemented.

- On the positive side, departments recognize that increasing expenditures on network services affords an opportunity to reduce other expenditures.

The net effect of pressures to reduce spending levels in the federal government is the same as that found in the private sector. Organizations recognize that increasing telecommunications expenditures affords an opportunity to achieve operating (cost) efficiencies. As a result, organizations have continued their spending for network services at rates somewhat higher than overall spending for information systems, but look for shorter term paybacks for any investments.

Policy and regulation are generally viewed as inhibitors, at least in the short term. Federal policies mandating use of FTS 2000 and government approved products retard growth in both telecommunications and network management products and services. In the longer term, they may turn out to be a positive force. When standards have been resolved and products are available, expenditures may increase for products and services that provide high quality management of enterprise networks. Accompanying the implementation of well managed enterprise networks will be even greater needs for data access and a flow of information.

Mandated use of FTS 2000 inhibits departments from moving forward with network development as aggressively as they would otherwise like. Recognizing that high-capacity services are not generally available through FTS 2000 inhibits some departments from moving forward. Many have opted to wait until services become available.

Interoperability, or lack of it, is a significant inhibiting factor. Federal government requirements for interoperable products is inhibiting many departments from developing new enterprise systems that make use of telecommunications facilities and services.

On the positive side, the demand for services such as EDI and E-mail is growing daily. Demand is expected to continue to grow, driving demands for increased connectivity throughout an organization.

The rapid progress of technology is stimulating the demand for new services and greater network capability. Until recently, organizations have had little choice but to implement and manage their own (local-area) networks. Technology is facilitating the growth of high-capacity (150+ Mbps) switched services that will be able to provide an alternative for local-area networking. Vendor provided, high-capacity switched services

will soon be available and may have an effect on the market for local-area network management products.

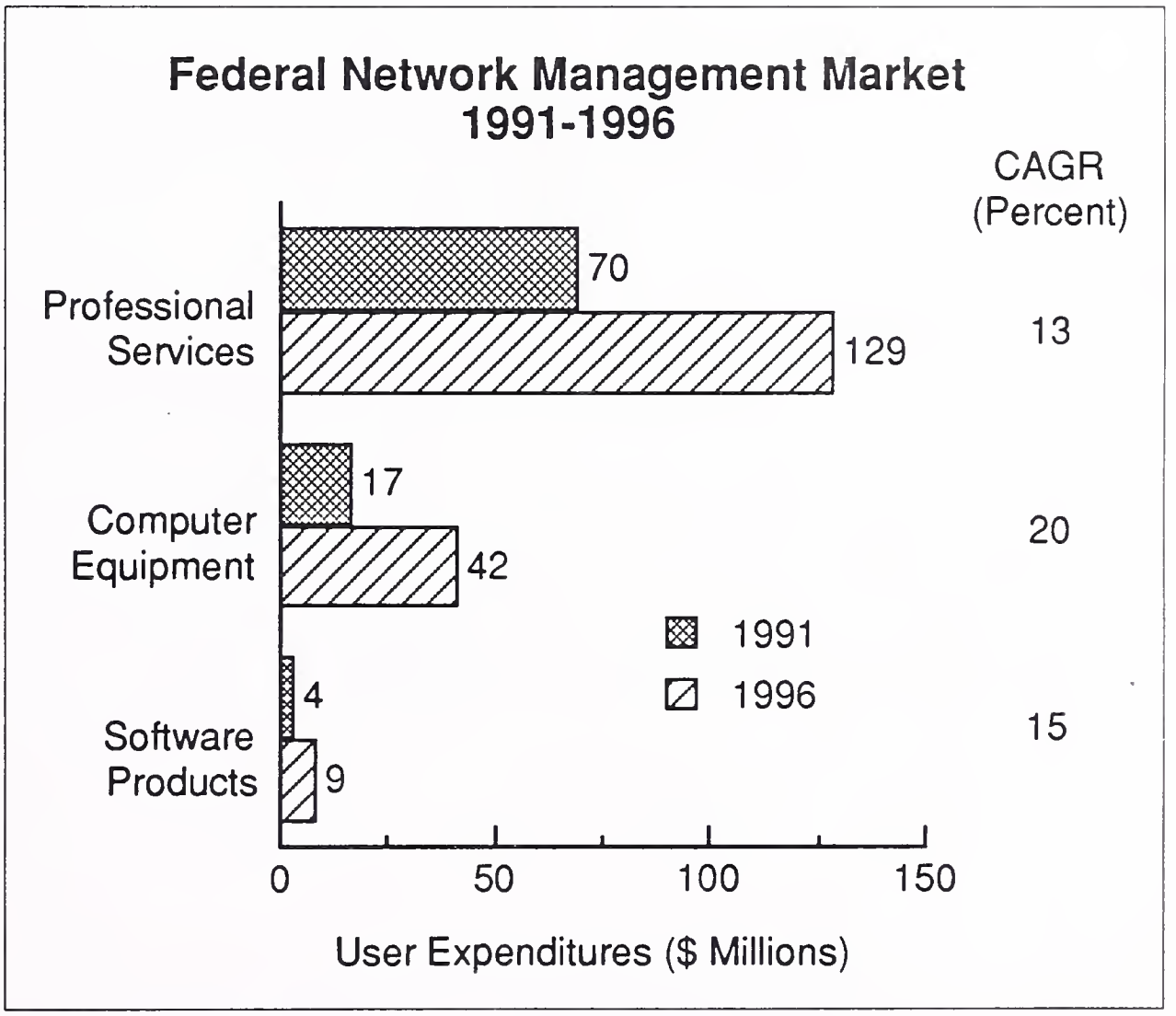
While technology is advancing, vendors continue to develop products that are incompatible and retard the development of interoperable systems. However, most recognize both the need and overall industry trends. Few, even dominant systems providers, will be able to continue to hold on to proprietary standards.

B

Market Forecast

As shown in Exhibit II-2, the federal market for network management products and services will grow from $91 million in 1991 to $180 million in 1996.

EXHIBIT II-2



Of the total, professional services will remain the largest, but the growth rate will lag behind hardware and software for the foreseeable future.

For the next several years, the greatest need will be for network management hardware to manage the growing number of integrated LANs. However, near the end of the five-year period, INPUT expects that greater attention will be given to managing enterprise networks. As enterprise

networks play a more prominent role in agency networking plans, greater assistance will be needed to identify methods to manage these complex networks.

C

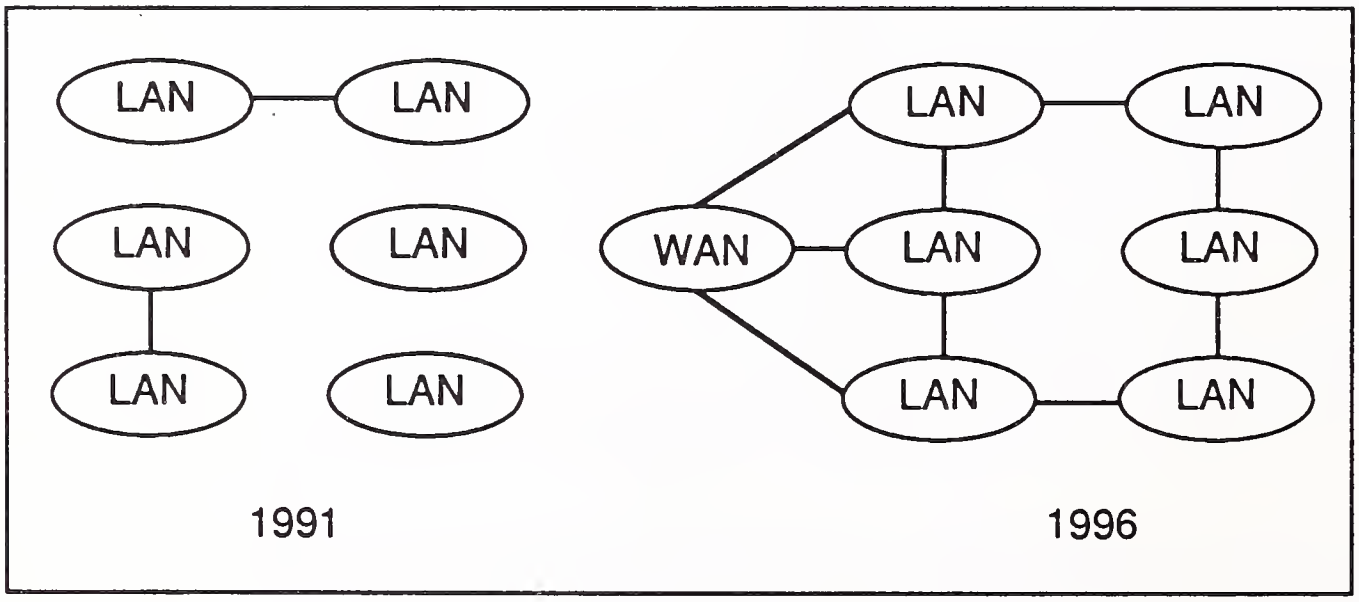
Federal Local-Area Networks

Local-area networks have not, as yet, achieved the status of a basic commodity, but the day may not be far off. Research for this report indicates that 90% of federal departments have implemented at least one local-area network. There are at least 5,000 LANs installed and the number will triple or quadruple within the next several years.

Although the number of LANs is growing rapidly, the number of LANs that are interconnected is only beginning to grow. Federal agency departments indicate that 84% of their local-area networks will be interconnected within five years. With the growth, there will be greater need for network management products and services. As shown in Exhibit II-3, federal LANs will migrate increasingly from one-to-one connections to one-to-many connections.

EXHIBIT II-3

Federal Local-Area Networks



At the same time the number of LAN-to-LAN connections are growing, there will be significant growth in the number of LAN-to-WAN connections. Federal departments indicate that only 26% of their LANs are connected to WANs today. This figure will grow to 75% within the next five years.

Ninety percent of federal departments manage their own LANs and two-thirds have installed network management products. The most frequently used is Novell. INPUT expects the percent of departments that manage their own LANs to remain high for the next couple of years, as the number of LANs implemented increases. However, as departments begin to connect more of their LANs to WANs and develop enterprise networks, the number will decline. Because of the greater amount of resources required to manage enterprise networks, departments will look for more cost-effective approaches.

D

Federal Wide-Area Networks

Federal departments indicate that there are more than 35,000 network circuits currently installed to meet agency-specific network needs. These are exclusive of department use of FTS 2000.

Like local-area networks, wide-area networks are managed primarily through in-house staff. Only 25% of agency-specific networks are managed through a contractor. Of those that are managed in-house, 50% are managed through formal network management centers.

While there are a large number of circuits installed, analysis of the circuit type suggests that agencies have, as yet, not begun to place significant emphasis on high-capacity networks. Of the total, only 7% are wideband (50 Mbps) or higher.

As departments place increased emphasis on enterprise networks, the percentage of high-speed circuits will increase and the percent of department contracting for (wide-area) network management services will grow. If the federal government's use of high-capacity circuits evolves similarly to that in the private sector, the percent of departments contracting for network management services should grow to 35-40% over the course of five to eight years.

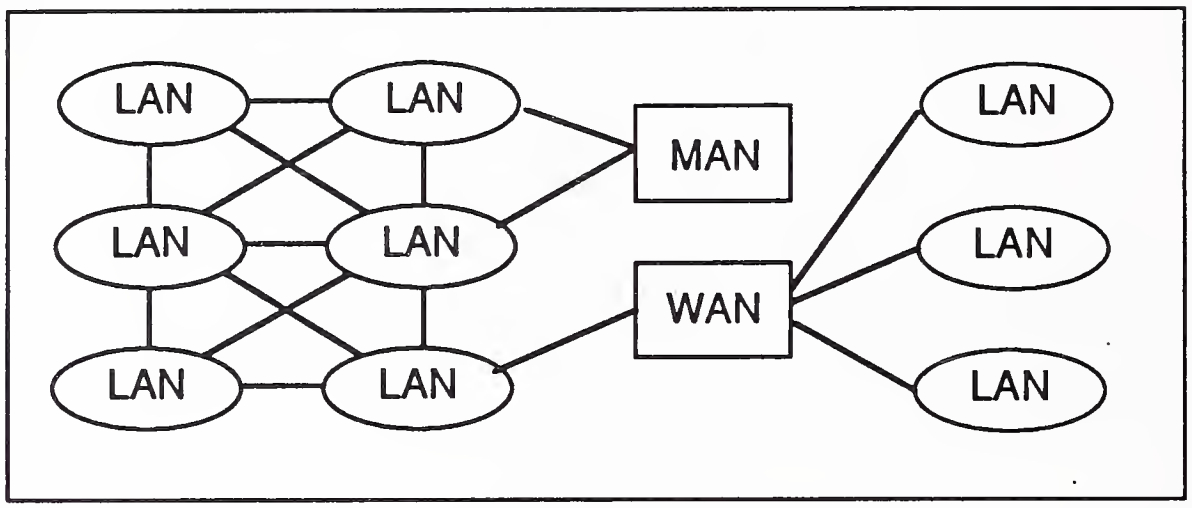
E

Enterprise Networks

Enterprise networking is clearly the direction in which private and public sector organizations are heading. Sixty percent of federal department respondents indicate that they have specific interest. Of those with interest, 88% believe that wide-area broadband-type networks are the most effective way to meet enterprise networking requirements. In the long term, INPUT expects federal agencies to migrate toward organization-wide connectivity, as shown in Exhibit II-4.

EXHIBIT II-4

Federal Enterprise Networks



LAN: Local-Area Network
MAN: Metropolitan-Area Network
WAN: Wide-Area Network

Although there is high interest in enterprise networking, INPUT believes that federal departments are overly optimistic in their plans for implementing such complex networks. Over 60% of federal department respondents indicate that they already have plans for enterprise networks and 60% indicate that they will begin implementation within the next year.

The process of developing and managing an enterprise network is highly complex. There are numerous management issues that must be resolved if the network is to be successful. INPUT believes that more than 60% of federal departments may have, in fact, begun planning and a few may take the initial steps to implement these networks. However, significant enterprise network development activity should not be expected for at least the next couple of years.

F

Federal Network Management

To date, federal departments have followed a path similar to that of the private sector for managing networks. Netview and Novell provide the most common wide-area and local-area network management products.

Twenty-five percent of federal departments contract for wide-area network management, a rate somewhat higher than private sector organizations have done in the past. Ten percent of federal departments contract for local-area network management.

Both of these percentages are expected to change. The federal government is expected to follow the general pattern of the private sector. As networks have become more integrated and complex, greater attention has been given to contracting with vendors that have the tools and expertise to manage networks. The federal government is not expected to be any different.

G
Recommendations

There are a number of recommendations that result from research for this report. To a great extent, they stem from two overall conclusions. The first is that the federal network management market is still immature. The second is that the market for comprehensive network management products and services will grow slowly in the short term and become a significant opportunity in the long term. Key recommendations are summarized in Exhibit II-5.

EXHIBIT II-5

Recommendations

- Educate users
- Focus on network planning
- Establish system/network vendor alliances
- Develop integrated network management solutions

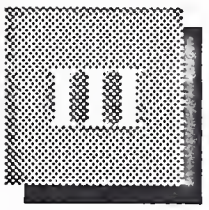
- There is a significant need to educate end users in both the benefits and problems of enterprise networking. Many users tend to view enterprise networking as an extension of establishing connections between several PCs and a printer.

- The major short-term need is to provide an architectural approach from which to grow. Strategic approaches need to be established before real interconnectivity can progress. Without an architecture strategy, many agencies could end up with piecemeal implementation that could be a management nightmare.

- Vendors of network management products and services need to establish alliances with hardware providers both to ensure a presence and to ensure an understanding of solutions that are possible. Without alliances, service vendors may lack technical knowledge of connectivity options.

- There is a particular need for integrated network management solutions. This need is not expected to abate until hardware vendors accept that interconnectivity is of greater value to users than vendor-specific protocols, no matter how much better the vendor's approach may be.

The market for integrated network management solutions is still young. Several years may be needed for the market to begin to mature. Successful vendors will establish relationships through consulting and education. These relationships will form a base for understanding system and network needs and for successfully addressing integrated network management requirements.



Market Analysis and Forecast

Growth of networks has been dramatic over the past twenty years. Users that were concerned about the availability and quality of basic voice services years ago are now concerned with how to improve the flow of intra- and inter-organizational information over increasingly complex networks.

Organizations that previously had concern about managing their voice systems now accept voice services as a basic commodity. As concern over voice systems decreased, issues began to arise about the availability, quality, and cost of long-distance (wide-area) networks (WANs). Although such concerns - particularly about quality and cost - have continued, organizations increasingly recognize that their networks are an asset.

With the emergence of workstations and PCs, local-area networks began to emerge. About the same time, local-area and metropolitan-area networks began to receive increased attention, particularly as users sought alternatives to high-cost carrier services to meet the needs of users in a building complex, a campus, or spread throughout a community.

However, local-area networks have generally grown haphazardly, not unlike the way wide-area networks grew in the early days. Users or departments of users frequently select networking capabilities that meet their needs, but do not take the organization's overall needs into account. This bottom-up approach may lead to incompatible systems. With the growth of disparate and specialized networks, the increasing recognition of networks as an asset, and the growth of systems integration, organizations increasingly realize that networks must be integrated to meet their future needs.

Unfortunately, many vendors have not fully accepted the changes taking place. The lack of acceptance is understandable, since their first priority is to sell products that are available today. In the future, vendors will need to accept that functionality is of far greater importance than a proprietary protocol.

Research indicates that the organization of the future will need to deliver information over integrated networks, most analogous to electronic highways. The highways will be comprised of very-high-speed circuits that permit users access to the network from a variety of entry points using a variety of means and equipment. With these integrated networks, there will be a need to accurately identify and respond to problems and to quickly identify design alternatives to ensure a continuous flow of information.

Until recently, network management was complex, but oriented to a single type of network. Circuit speeds were generally available within a fairly narrow range. Terminals were (predominantly) dedicated and network volumes were identifiable.

With the advent of local-area and wide-area networks, diagnostic and management considerations began to change. Circuit speeds are orders of magnitude higher and the volume of data is both unknown and generally unpredictable. Greater attention must be given to the integration of networks with applications. And, as network speeds increase, more sophisticated management tools become necessary.

Most users still focus on integration of local-area networks and identifying improved network management tools, but users are beginning to become interested in developing networks that result in an electronic highway for an entire enterprise.

Many issues in developing an enterprise network are management issues and many recognize that managing an enterprise-wide network requires considerably greater effort and more sophisticated management approaches and tools.

When considering network management, the federal government is no different than the private sector. The networks of each are increasingly complex. Each recognizes the importance of networks to the organization and each is considering alternatives for managing integrated networks.

This chapter discusses the overall market structure for networks and network management products and services, and provides an analysis of the market for network management products and services. The network management product and service market is discussed for local- and wide-area networks and a preliminary assessment of the market for enterprise network management is provided.

A
Market Definition and Structure

To understand the growing importance of networks and network management, several factors must be taken into account, since they have a direct bearing on the size of the market for network management services and the approach taken to penetrate the market.

The first factor is the definition of a telecommunications network. INPUT defines a network as *electronic interconnections between sites or locations that may incorporate links between central computer sites and remote locations and switching and/or regional data processing nodes*. When considering the definition, there are several points to keep in mind.

- The definition encompasses data, voice, video, and textual information.
- The definition excludes applications software.
- The definition includes service delivered over dedicated (leased) facilities and delivered over switched facilities.

Consideration must also be given to the definition for network management. INPUT defines network management as *contracting for the management of all or a significant portion of a network under a long-term contract*. This definition generally refers to a specific contract for management services for an extended period of time. As part of the contract, the vendor provides necessary hardware and software.

The definitions are noted because they reflect both the growing complexity of networks and the difficulties that many organizations (federal and commercial) will have in managing enterprise networks. Networks of the future will be utilitarian in nature, requiring management of a variety of services that have vastly different operating characteristics. Many organizations will be unable to afford to provide the breadth of skills necessary to manage these networks.

For the purpose of this report, INPUT's definition has been broadened to include software and hardware acquired by agencies to manage their own networks. The forecast provides a breakdown to show the portions that relate to INPUT's (traditional) definition and the portions that relate to acquiring products for an organization to manage its own network(s). The following summarizes the types of products and services included in and excluded from INPUT's forecast of the federal network management market.

- *Included*
  - Voice networks
  - Data networks
  - Hardware
  - Software
  - Maintenance

- *Excluded*
  - Internal management costs
  - Regularly tariffed services

Regularly tariffed services are network management services provided on an ongoing basis as part of a customer's basic service cost. The most notable example is Centrex service. With Centrex and other services such as FTS 2000, network management is bundled into the basic (tariffed) service charge. Bundled (network management) service costs are excluded from INPUT's network management forecast.

B

Federal Networking

As noted elsewhere in this report, INPUT believes that the market for federal network management products and services, particularly integrated ones, has yet to begin to grow. Key reasons can be found by understanding fundamental differences between local- and wide-area networking. The differences serve as a baseline for understanding needs and requirements for developing enterprise networks and tools to manage them.

Exhibit III-1 provides a comparison of a number of key characteristics of local- and wide-area networks. The differences form the base for issues that must be resolved for federal agencies to successfully manage networks of the future.

EXHIBIT III-1

WAN/LAN Characteristics

	WAN	LAN
Data Type	Data	Information
Access	Controlled	Limited control
Volume	Predictable	Unpredictable
Changes	Controlled	Uncontrolled
Speed	2.4-9.6 Kbps	150+ Mbps
Security	Network specific	Limited

- *Data Type* - Data networks transmit data. While larger, general purpose networks can permit certain amounts of text, the volume is small and transmissions are generally of known composition. Transactions have predefined fields with fixed, maximum numbers of characters.

  A local-area network has no specifically defined type of data. Most transmit a combination of data and information. Unlike a data network, there is no definable composition of transmissions. Users accessing a host system one minute may be sending a flood of messages the next. Data to update a data base may be followed by transmission of an image or a large spreadsheet. Each has different data characteristics.

- *Access* - Access to data networks is centrally controlled. Designers know in advance the location and type of access devices. While any device may or may not be active at any given time, the highest level of activity can be predicted. Generally, changes can not be made without prior knowledge.

  From a management sense, access to resources from a local-area network is generally uncontrolled. Selective restriction is, at best, difficult. Once networks are integrated, users generally have access to all other users and systems on the network.

- *Volume* - The volume of a data network is predictable. With experience and the use of design and management tools, volume by hour, day, or month can be predicted. Networks can be designed to accommodate the highest predicted volume.

  Unlike a data network, the volume of data/information on a local-area network is both unknown and generally unpredictable. Once implemented, network monitoring will result in profiles that can be applied to future development, but in the short term, there is little data that can be used to determine average usage by hour or day.

  Of more importance when considering local-area network volume are the dynamics of information flow within an organization. Unlike data networks, there is little data to suggest when managers and staff send messages, what data is needed when, or the characteristics of data transmitted or received. Because of the unpredictability, local-area networks must be designed to provide exceptionally high bandwidth to meet a wide variety of transmission requirements.

- *Changes* - Changes to a data network software are strictly controlled. Systems, network, and operations planners must know at all times which terminal device interacts with which piece of software. Changes made to one piece of software could affect the operations of all devices on a network. Changes are pre-planned, scheduled, and carefully monitored.

Changes to software on a local-area network are difficult to control. Software run on PCs and workstations is acquired by individuals to meet individual needs. With the exception of standards for word processors or spreadsheets, users of departments have varying needs for software products. Changes made to software at one PC on a network can have a significant impact on the performance of the network.

- *Speed* - Compared to local-area networks, data networks operate at low speed. Most data transmitted from a computer ranges in speed from 2.4-9.6 Kbps. Multiplexers permit the combining of transmissions onto higher speed circuits. Fiber and T1 circuits permit the combining of numerous low-speed circuits. But in each case, a computer transmits or receives the data at the much lower speeds.

  The speed at which local-area networks transmit is dramatically different. Networks transmitting at 150 Mbps and above are more closely associated with channels on a computer system than traditional data networks. There are few tools available to provide comprehensive analysis of LAN transmission characteristics.

- *Security* - Security for data networks is generally specific to a network. Networks that require high security are separated from general application networks. The necessary degree of security is applied in each case.

  Unless multiple local-area networks are established, security is a significant issue. Most users will not contend with the requirements of a high-security network. Security issues become significantly greater as local- and wide-area networks are integrated into enterprise networks.

C

Managing Enterprise Networks

The technical and functional differences are important considerations, but there are a number of equally important questions related to the purpose for establishing enterprise networks.

For many organizations, there is sufficient technology available to meet most needs. However, few organizations have, as yet, addressed important management issues. These issues relate fundamentally to the purpose and control of an enterprise network.

- Is the purpose of an enterprise network to transmit data and only data directly between PCs and workstations and only PCs and workstations?

- Should all user terminal devices (PCs, workstations, terminals, etc.) have access to all computing resources, including mainframes and other terminals?

- Should the network provide a common electronic highway for the transmission of all corporate media (voice, data, text, visual)?

- Are all users permitted to have access to all agency information or only subsets? If subsets, which subsets will be accessible by which individuals? And who controls access permission - the agency, information systems, or must department senior management make the decisions?

- What about software standards? Can an agency set (and enforce) standards that limit users to a choice of two word processing packages, one spreadsheet, and one desktop publishing package?

Compounding the issues of what is to be accomplished by an enterprise network and the technological issues surrounding the differences between traditional local- and wide-area networks, there can be significant differences in data and information requirements within an organization and between organizations.

The differences in data and information needs can have a major effect on network design, development, and management practices, policies and tools. Key management considerations include those summarized in Exhibit III-2.

EXHIBIT III-2

Key Management Considerations

- Staff requirements
- Management requirements
- Information dissemination
- Information/data security

- *Staff Requirements* - In most organizations, department staff require data. Their primary function is to receive, analyze, and synthesize data into meaningful information. Depending on organizational requirements and the availability of data, department staff will access a number of data bases (some internal and some external) to obtain the data. There can be extensive interaction between individuals working with the same data, requiring multiple transmissions of high volumes of data.

  Within certain bounds, data needs can be anticipated. Accounting department staff perform extensive analysis at the end of defined periods (week, month, quarter, etc.). However, research and planning staff continually need a wide variety of data. Their needs are irregular and generally unpredictable.

- *Management Requirements* - Management receives and disseminates information. Its needs are irregular and unpredictable. Changes in events may cause immediate, comprehensive data analysis by staff. Whether received from staff or created internally, information distribution must frequently be immediate and widespread.

- *Information Dissemination* - Dissemination of data and information may be narrow (one-to-one) or wide (broadcast). It may be internal or external. Information to be distributed may be highly restricted or intended for general release. Release of confidential data can be highly damaging. This unpredictability results in concern about security, priority, and potential impact on other systems.

- *Information/Data Security* - Much information and data in an agency is highly confidential. Extensive linking of LANs imposes significantly increased security considerations. How will security be controlled? How will information flow from a secure to an unsecured network? How can an enterprise network be effectively secured without restricting information flow between individuals with a need to know?

INPUT believes that most agencies have not yet begun to address the complexities associated with developing and managing comprehensive enterprise networks.

The complexity of developing enterprise networks affords opportunities for vendors. Technologically oriented managers in many agencies are not fully aware of the complexities. Many will need assistance in identifying requirements and developing plans.

D

Market Forecast

INPUT's forecast for the federal network management market has been developed recognizing the complex technical and management issues that federal agencies must address. The forecast also considers the nature of enterprise networks and the wide variety of network management options open to agencies.

Enterprise network service may be provided over dedicated or switched service facilities or a combination of facilities. Because of the (integrated) nature of an enterprise network, network management services may be provided in several different ways at the same time.

- An agency may contract with a vendor to manage the entire (local- and wide-area) network.

- An agency may contract with a vendor to perform maintenance service for remotely located equipment, but retain overall management responsibility and control.

- Network management service may be provided by a vendor as part of the provision of a portion of an agency's circuits. The agency retains overall management responsibility and control.

- An agency may contract with a vendor to manage the agency's entire enterprise network.

A forecast for the enterprise network management market must acknowledge several points.

- Combining networks will tend to reduce the market for products related to a specific type (LAN or WAN) of network.

- An enterprise network is considerably more complex than either a traditional wide-area (data) or a local-area network. Combining different types of networks into a single electronic highway requires more in-depth analysis and more comprehensive management tools.

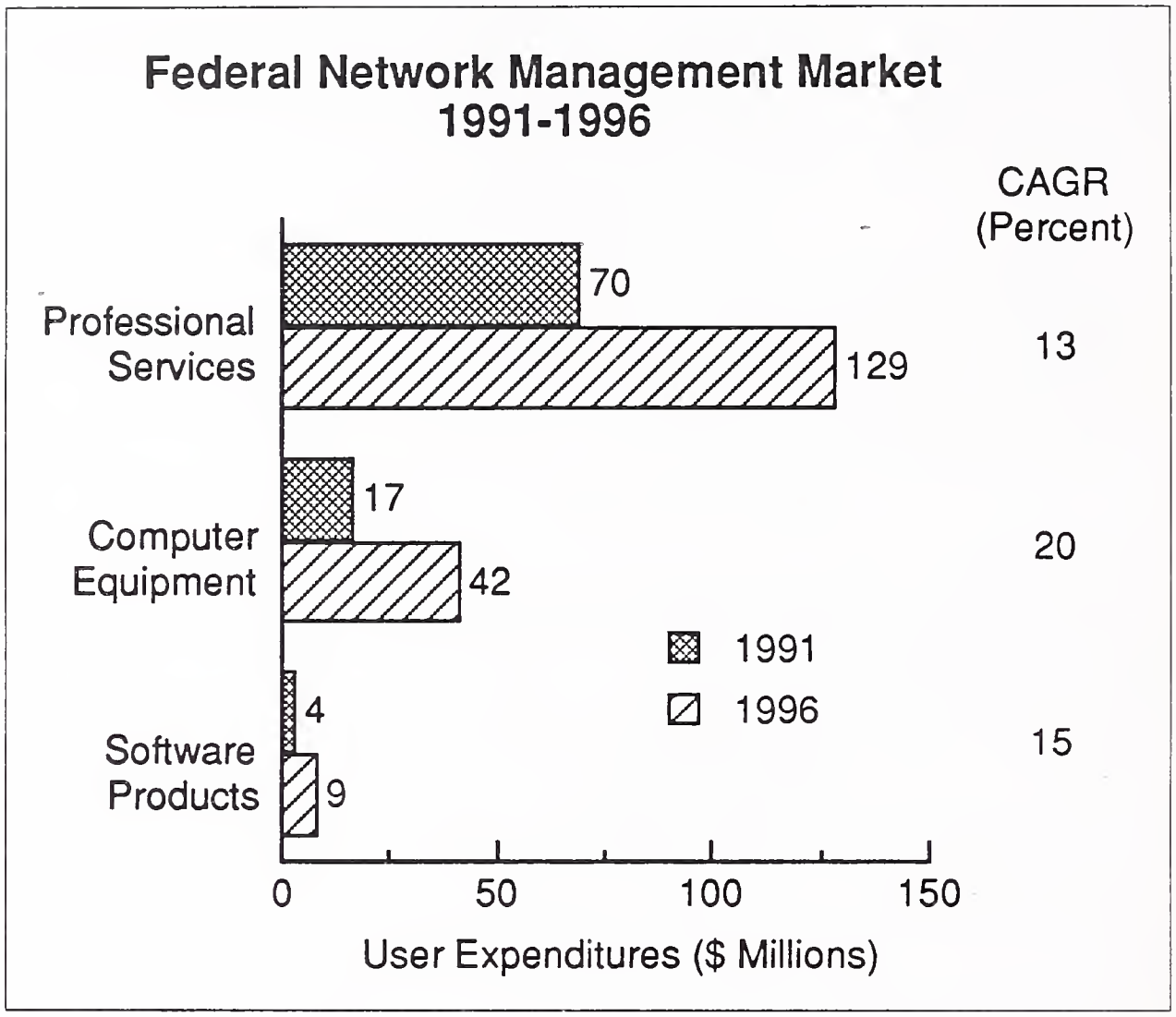
- The market for enterprise network management must be considered a new market. Enterprise network management products are only beginning to emerge. Substantial growth may not be realized for the next two to three years.

- For many agencies developing comprehensive, enterprise networks, the only really viable management option will be to require that a single vendor be responsible for management of the entire network. Few organizations have either the skills or products to manage an enterprise network.

Exhibit III-3 provides a summary of the market for network management products and services in the federal government. Overall, the forecast reflects continued focus on products and services for managing disparate networks in the short term. In the longer term, the market will evolve into more integrated products and services and greater emphasis on contracted network management services. The contracted services will be more closely in line with INPUT's definition of network management.

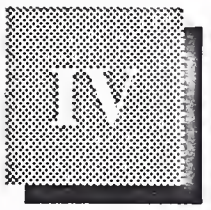
As Exhibit III-3 shows, the federal market for network management will grow from $91 million in 1991 to $180 million if 1996, a CAGR of 15%. Growth in the professional services category, while remaining the largest, will lag behind the other categories. As shown in the next chapter, most agencies intend to manage their own networks, without using a contractor.

EXHIBIT III-3



While this will hold down the growth of professional services, it will give a boost to the two product categories. As networks become more complex, agencies will require more and better hardware and software to manage them.

Overall, INPUT expects the market for network management products and services to be a dynamic market. The market will continue to be focused on products and services for single, disparate networks in the short term. Nearing the end of the five-year period, the market will begin to shift to integrated products and services to manage complex enterprise networks.



Federal Network Management

As noted in the introduction, a key focus of this report is the evolution of federal networking from dedicated use local- and wide-area networks to enterprise-wide networking. Chapter IV discusses the types of networks currently implemented, methods used of managing local- and wide-area networks, and federal agency interest and plans to develop enterprise networks. These are followed by a discussion of the primary approaches currently used to manage LAN and WAN networks and requirements for successfully managing enterprise networks.

A Wide-Area Networks

In general, the federal wide-area networking environment is not much different from the environment in the private sector.

Though the technological demographics may be different, federal networks are connected to similar types of mainframes. The reasons behind their evolution are fundamentally the same, and the federal government and the private sector are faced with the same network management problems.

1. Connection Methods

In INPUT's 1990 report on the federal telecommunications market, user data indicated that an estimated 67% of agencies have agency-specific networks. Respondents indicated that they would be generally inclined to obtain future data networking services through FTS 2000. As a result of the switch to FTS 2000, only an estimated 26% of the agencies would have agency-specific networks by 1995.

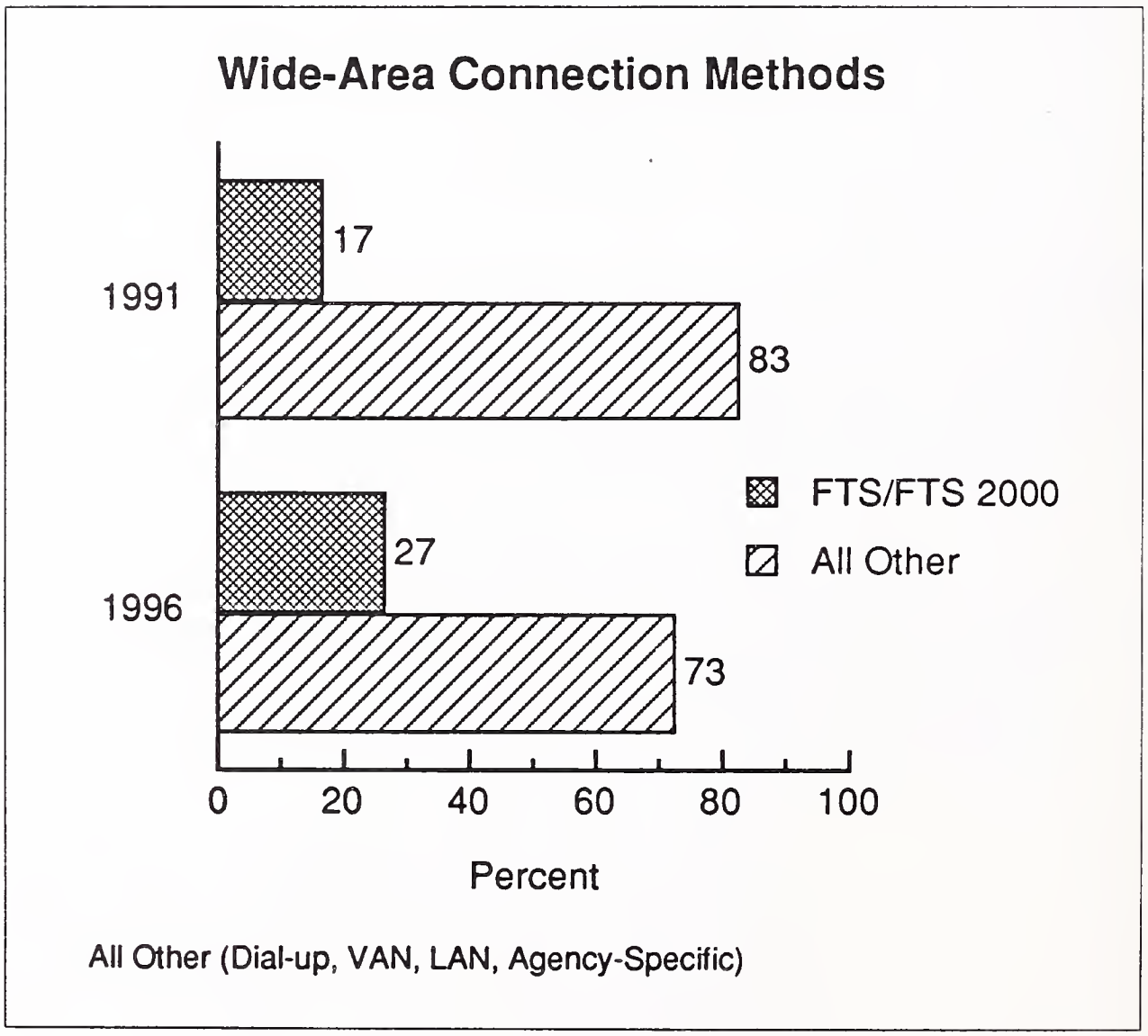
Research for this report resulted in data suggesting that the rate of conversion to FTS 2000 may not be as high as originally anticipated. As shown in Exhibit IV-1, results of research for this report suggest that a very high proportion of agency networks will remain agency-specific. Though

concern about the ability of FTS 2000 to meet data networking needs has been expressed, INPUT believes that the difference results from two primary factors.

- The first factor is a somewhat different composition of respondents. For this report, there was a higher proportion of technologically oriented organizations. Organizations involved in science and engineering frequently have much greater needs for very high-speed networking capability. They can be expected to be somewhat critical of the ability of FTS 2000 to meet their needs.

- The second factor is a growing recognition by a number of agencies that they will need higher bandwidth to meet their needs than is currently available through FTS 2000. Whether FTS 2000 will be able to provide very high bandwidth is open to question.

EXHIBIT IV-1



As an indication of the trend toward high capacity and the possibility that resistance to converting to FTS 2000 could grow, consider the requirements of the Army Corps of Engineers. Such organizations show a reluctance to convert sophisticated networks to networks such as FTS 2000 which cannot currently meet their needs.

The Corps has a complex campus-wide (local-area) network using FDDI technology. The Corps' network consists of three separate FDDI network rings connecting 23 buildings on a 700-acre campus. The network provides access for scientists and engineers from workstations and PCs to DEC and Cray Research systems. The Corps has adopted FDDI as its preferred network type, but believes that, in the long run, it will need network speeds that exceed FDDI speeds by as much as 8 to 10 times.

Although the Corps' networking needs exceed those of many commercially oriented (federal) organizations, its interest in broadband, wide-area networks reflects the interests of many users. As noted later in this chapter, federal agencies believe that broadband, wide-area networks similar to this will be needed to support enterprise networking needs in the future.

This example is not intended to suggest that FTS 2000 is somehow lacking by not being able to meet the Corps' needs. FTS 2000 was not intended to meet local-area networking needs. The example is provided to illustrate the trend of many federal organizations toward higher and higher speed networks, both locally and nationally. Many question whether a utility network such as FTS 2000 will be able to meet the very high bandwidth needs of the future.

As part of the research for this report, INPUT sought to identify the extent of agency-specific (wide-area) networks currently implemented. In total, more than 1,000 federal government sites indicate that there are more than 35,000 agency-specific network circuits installed.

The actual figure must be viewed with considerable caution, since multiple sites are counting the same circuit. However, the high number clearly indicates that there are a very high number of agency-specific networks currently installed. While many agencies may be interested in obtaining circuit services through FTS 2000, the number of departments indicating that they will be using agency-specific networks five years from now (73%) suggests that the process of conversion will be, at best, lengthy. Concerning network management, there are two additional points to note.

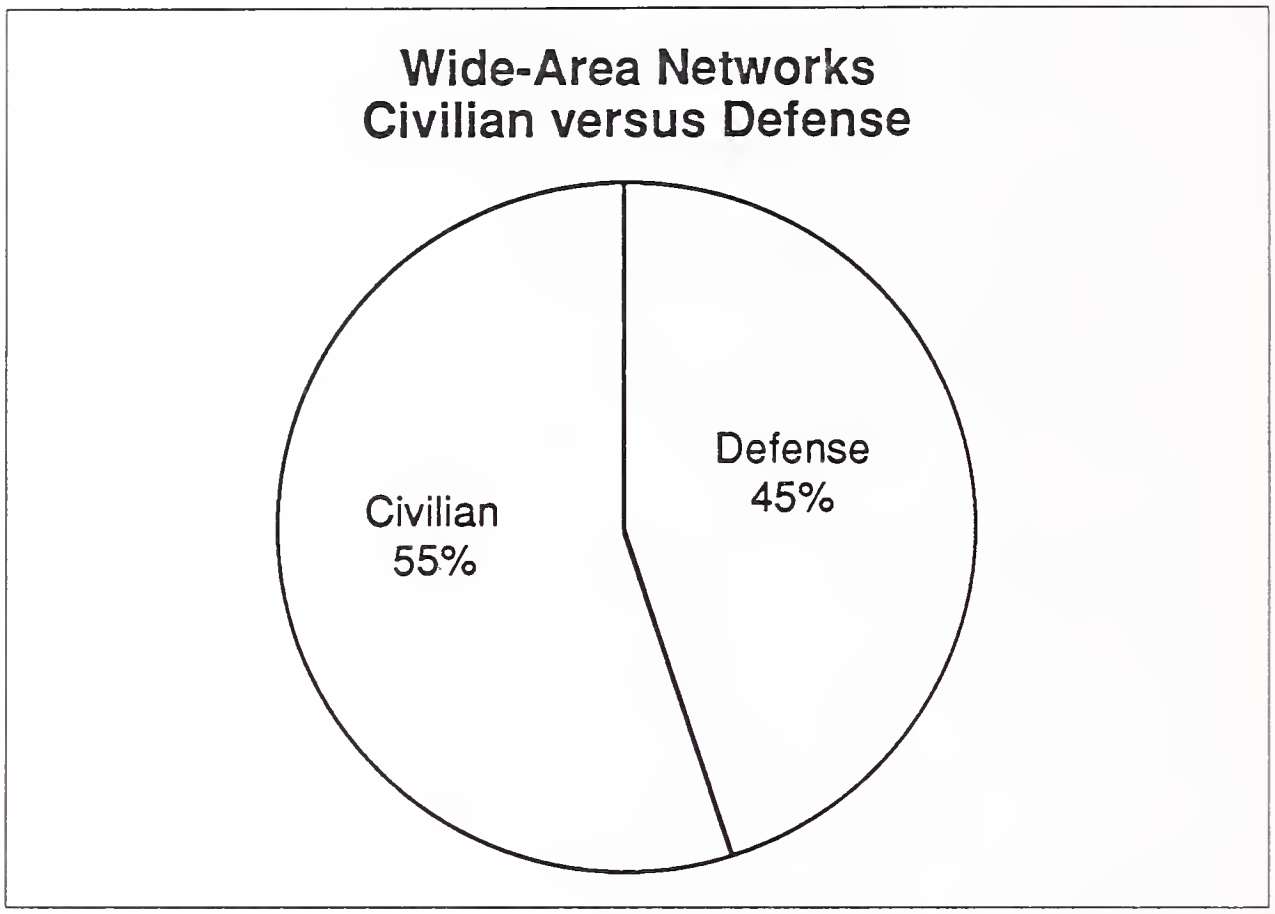
- The data suggests that there will be a requirement for organizations to manage their own networks for some time to come.

- Network management requirements will increasingly involve high-speed (LAN type) networks.

2. Defense/Civilian Networks

As might be expected, an estimated 45% of department networks support the Defense Department, as shown in Exhibit IV-2. Within the Defense Department, the Navy reports the highest number of circuits (6,500), followed by the Army (5,000).

EXHIBIT IV-2



Although civilian departments account for 55% of the total number of circuits, few agencies have extensive networks. Exhibit IV-3 identifies the number of wide-area network circuits for the leading civilian departments. However, it should be noted that these networks are frequently concentrated within several large departments. Many agencies have little wide-area networking capability.

EXHIBIT IV-3

Wide-Area Network Circuits
Leading Civilian Departments

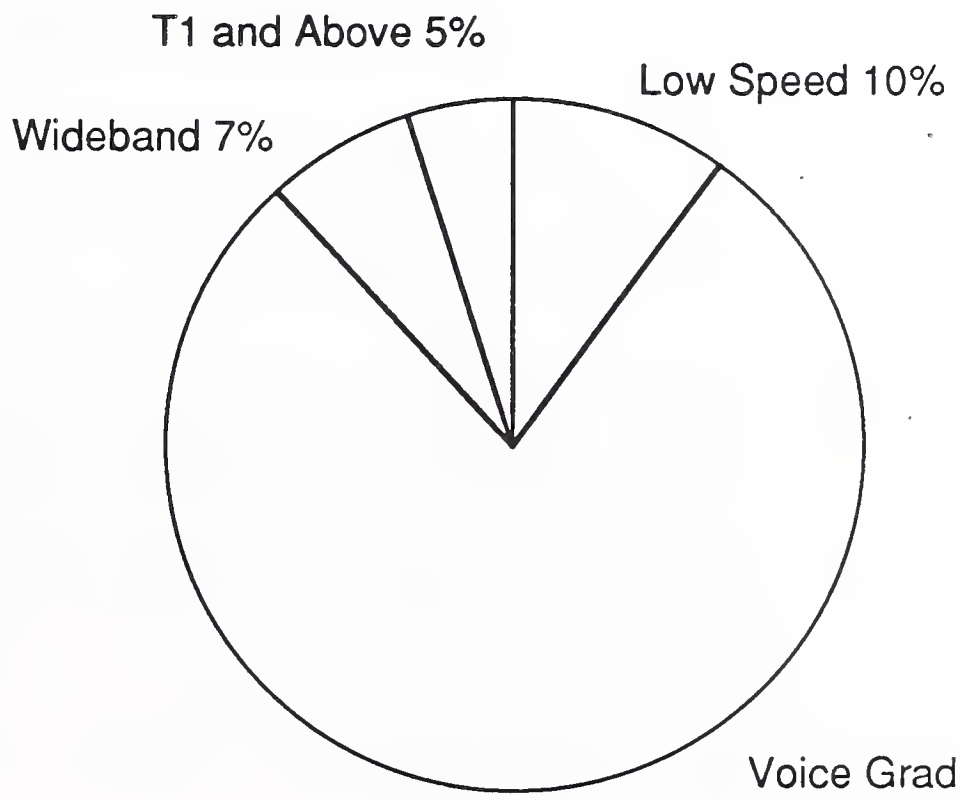
	Number Reported
Energy	2,480
Postal Service	1,830
Veteran Affairs	1,825
Health/Human Services	1,500
NASA	1,415
Treasury	1,200

3. Network Types

The types of agency-specific networks are consistent with the mix that would be found in the commercial sector. As shown in Exhibit IV-4, voice grade circuits are the predominant circuit type. This is not expected to change in the short term, but an increasing number of organizations are placing greater attention on wideband and higher speed service.

EXHIBIT IV-4

Federal Wide-Area Network Types



Notes:
Low Speed:	300-1200 bps
Voice Grade:	1200 bps to 9.6 Kbps
Wideband:	56-256 Kbps
T1:	1.5 Mbps

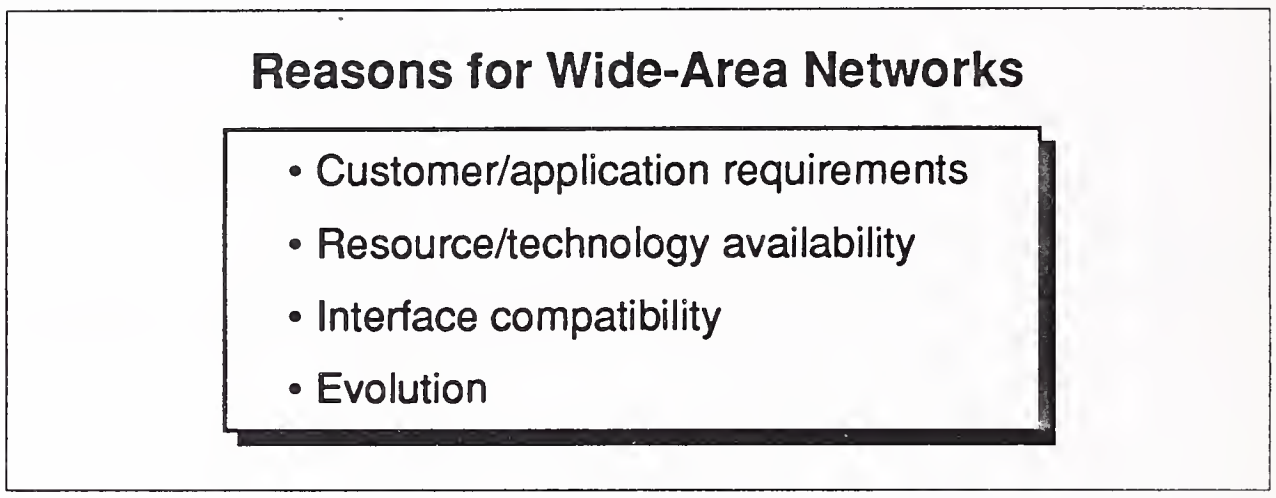
It's important to note that an estimated 10% of federal wide-area circuits are low speed. Low-speed circuits frequently use analog transmission technology and integrating these into high-speed enterprise networks can pose some significant challenges. Equally important, the equipment used on lower speed networks is frequently incompatible with newer network technologies. This suggests that a high number of terminals that must be changed to be able to make use of higher speed (integrated) networks.

4. Wide-Area Network Reasons

Although future needs will include high-capacity, integrated, local- and wide-area networks, today's networks have been developed to meet

specific user and technology needs. Exhibit IV-5 identifies common reasons why wide-area networks have evolved as they have.

EXHIBIT IV-5



In nearly all organizations, wide-area networks have grown in response to customer needs for specific applications. In most cases, wide-area networks have just *evolved*, frequently with little thought about the long-term financial or operational impact.

The evolutionary process is not surprising, considering that early networks were not terribly reliable. Users funding one application did not want their work impacted by work being done for another application. Until recently, one large commercial organization had more than 150 different wide-area networks supporting different applications. The networks served the same geographic area and most of the end points were the same.

The federal government is not significantly different. Wide-area networking has evolved to support specific applications. As the need grows to support integrated applications, integrated networks are necessary. Integrated networks become necessary not only to achieve cost savings and operational efficiency, but also to provide the means for data sharing across wide geographic areas. The term *integrated networks* increasingly refers to local-to- wide-area connectivity.

Vendors of network and network management products need to recognize that applications will continue to be drivers behind the evolution toward integrated networks. Organizations that do not integrate their systems typically have little need for integrated networks. Organizations developing integrated data bases and complex applications such as imaging and geographic information systems will have the greatest need for high-speed, integrated networks. They will also have the greatest need for comprehensive network management systems.

B
Local-Area Networks

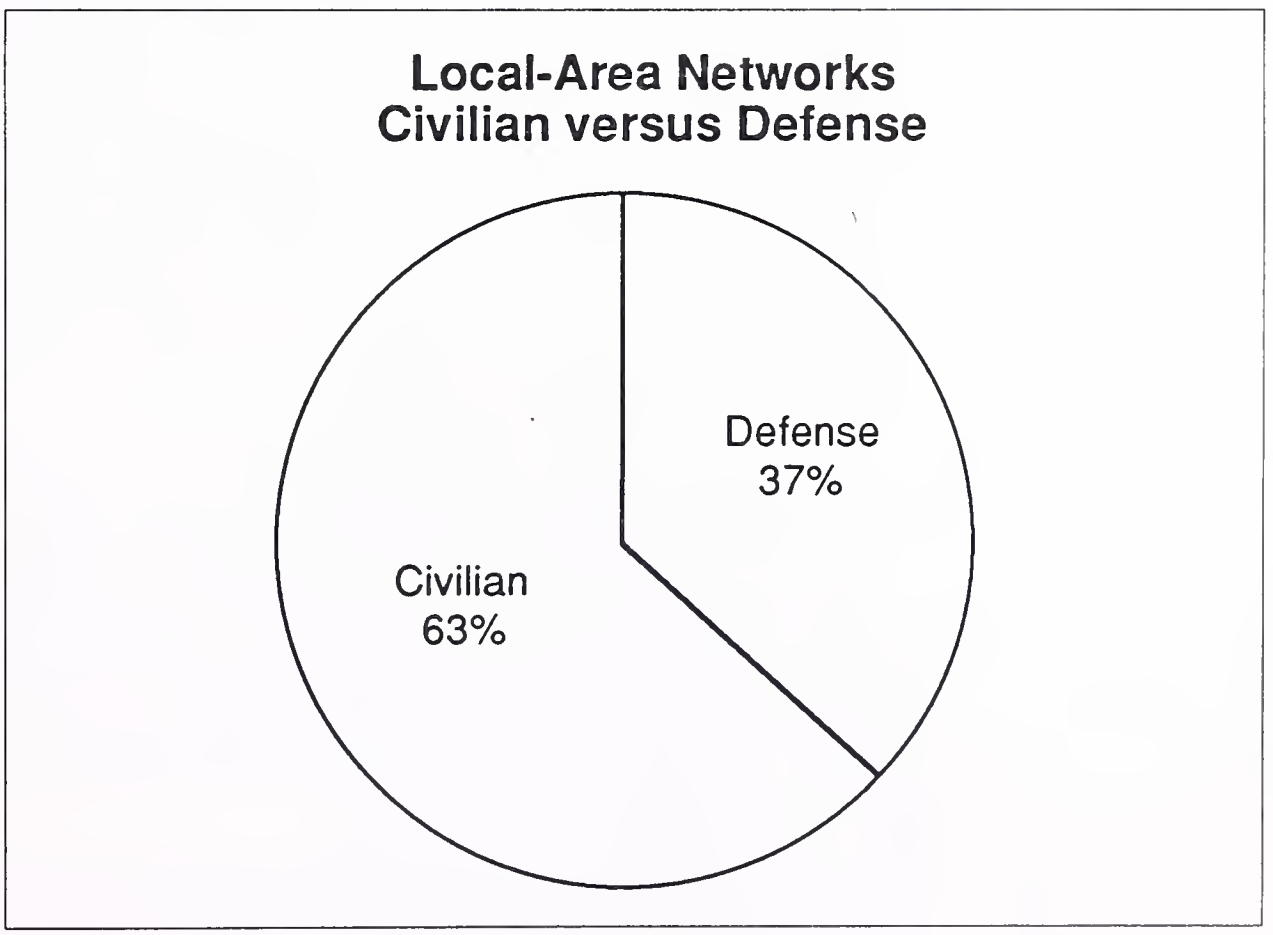
1. LAN Network Types

Since local-area networks' introduction several years ago, they have become somewhat commonplace. LANs are becoming as common in federal offices as typewriters and copiers. Some foresee the day when they will be as necessary to the success of daily operations as electricity. However, until recently, most local-area networks were implemented in isolated islands, providing connections only between several workstations or PCs in a department or work area.

LANs have not, as yet, achieved the status of a basic commodity, but the day they do may not be far off. Research suggests that there are a minimum of 5,000 different LANs already implemented. Ninety percent of federal sites contacted in a recent survey indicate that they have at least one LAN implemented.

However, this represents a small portion of those that will be implemented over the next several years. As shown in Exhibit IV-6, the majority of local-area networks are in civilian departments.

EXHIBIT IV-6



Of the total LANs implemented in civilian departments, the majority of those specifically identified are Ethernet, as shown in Exhibit IV-7.

EXHIBIT IV-7

Local-Area Networks
Leading Civilian Departments

	Percent by Type			
	Ether	Token	FDDI	Other/Unk
Energy	43	7	10	40
Veterans Affairs	26	3	27	43
NASA	57	2	28	13
Health	36	7	7	50
Federal Reserve	82	8	-	11
Transportation	61	5	2	32

It's interesting to note that many users are not aware of the exact type of LAN implemented. In many departments, as many as half the individuals contacted did not know what type of networks were in use. The high incidence of 'unknown' responses may be considered good or bad, depending on the point of view.

On the one hand, LANs may be becoming sufficiently commonplace that people give little attention to the type. In this sense, LANs are becoming another utility, like heat or water. On the other hand, the lack of knowledge gives rise to concern about the effort and knowledge necessary to integrate and manage different types of networks. To effectively manage integrated networks, the attributes of each network and network elements must be known.

The high incidence of 'unknowns' suggests that vendors will have a difficult time developing enterprise networks and greater difficulty identifying and implementing network management products and services. Unless all network types and components can be identified, network management products that are selected will work with only a subset of an agency's networks. Recognizing the difficulty, many agencies may elect to wait for more standardized network management products before moving ahead.

The primary reason cited for Ethernet preference is that it is easier to implement and integrate with higher speed (FDDI) network environments. Several users have suggested that they believe that Ethernet will be easier to integrate into broadband wide-area networks, when these are available. Though vendors may question the validity of the belief, agencies believe that this is the case and are structuring plans based on the belief.

However, it should be noted that there are other types of networks, adding to the complexity of developing enterprise networks. Networks supporting Apple computers are common, and the Food and Drug Administration, NASA's Goddard Space Flight Center, the Labor Department, and the National Science Foundation have all implemented XNS (Xerox Network Services) LANs. XNS users indicate that integrating their networks into enterprise networks, particularly those based on TCP/IP architectures, will be difficult.

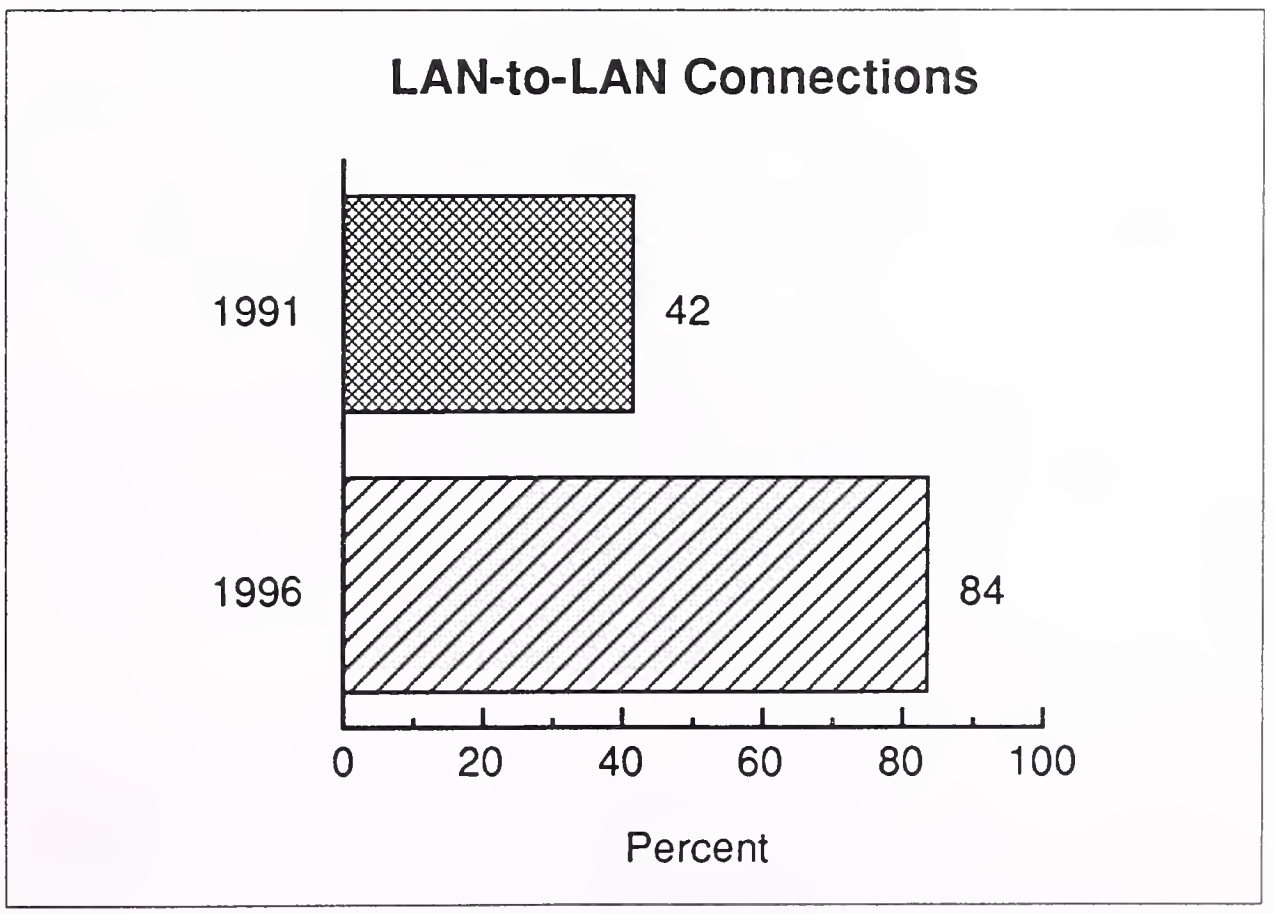
2. LAN-to-LAN Connections

Since the majority of federal agencies note that they have implemented local- area networks, research for this report placed emphasis on the extent to which agencies have begun to establish connections between more than two other LANs. The choice of two was somewhat arbitrary. In a large agency work group, there may be several LANs.

The purpose of the question was to assess whether agencies are beginning to move beyond the implementation of disparate islands and connect LANs together. Connecting more than two would indicate that connectivity is occurring between work groups rather than just within work groups.

As indicated in Exhibit IV-8, agencies have, in fact, begun to move beyond individual, disparate islands. Over 40% of the respondents indicate that their agency has established connections between two or more other LANs.

EXHIBIT IV-8



More importantly, departments recognize that establishing connectivity between LANs throughout an organization is a high priority. Eighty-four percent of respondents indicate that they will have connections between two or more other LANs within the next five years.

While the data suggests high inter-LAN connectivity today, INPUT believes that the 42% figure must be viewed with some caution.

Taken at face value, the figure could suggest that nearly half of the local-area networks in an agency are interconnected. INPUT believes that the figure does reflect a growing trend toward connecting LAN networks, but that the majority of those connected are typically within a confined work area.

Most agencies follow a typical progression of developing LAN interconnections. First, they connect several PCs and workstations within a work area. These generally share printers and sometimes files. Once terminals are connected, organizations begin to connect LANs together, but the LANs are still generally within a work area. These types of connections are followed by consideration of inter-agency connections.

INPUT believes that intra-work group connections are the predominant type of connections. Few organizations, either federal or commercial, have progressed to extensive inter-agency local-area network connections. Even fewer organizations have progressed to developing enterprise-wide, any-to-any LAN connectivity. However, as data sharing becomes more common and necessary, enterprise-wide connectivity will increase.

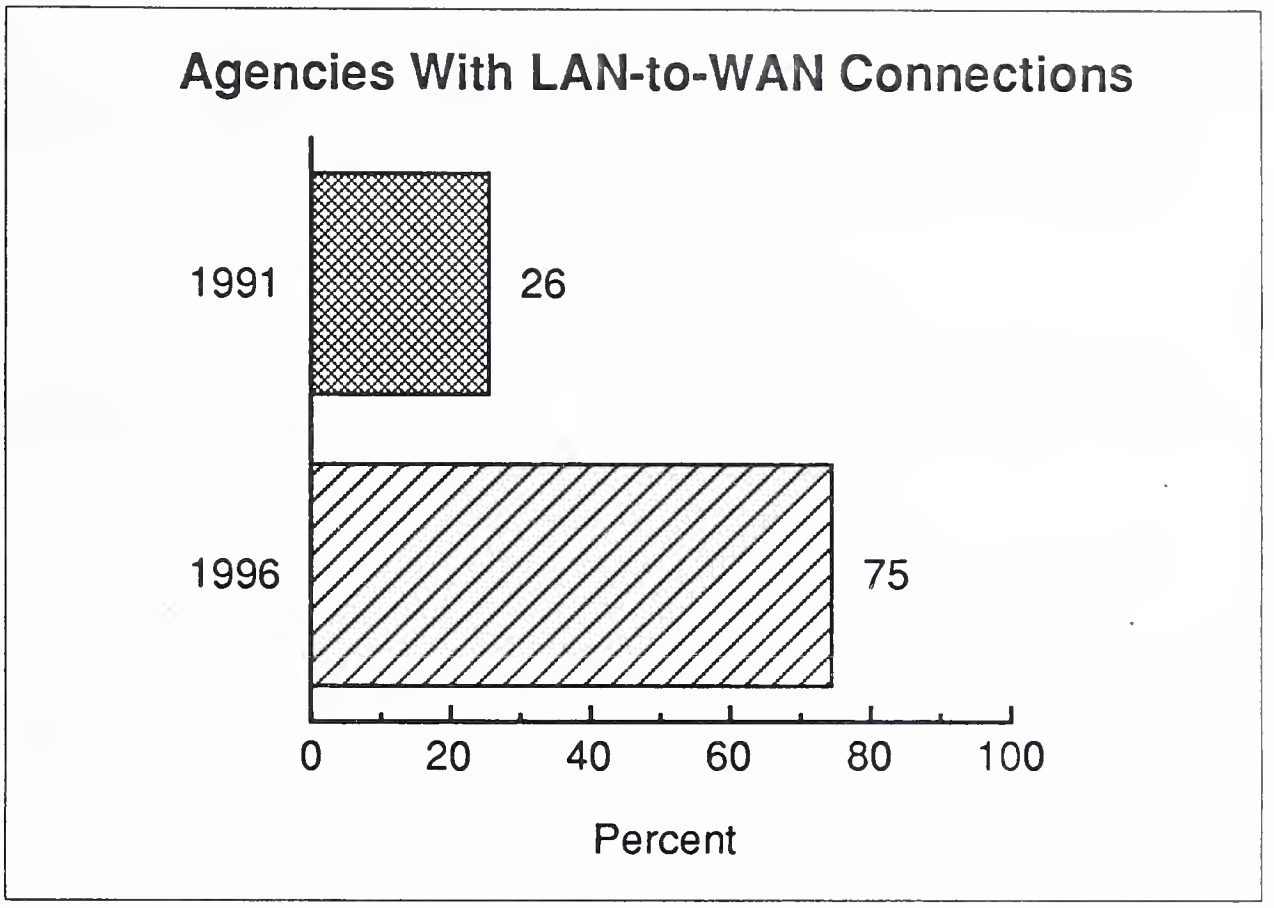
3. LAN-to-WAN Connections

While organizations appear to be progressing with LAN-to-LAN connections, LAN-to-WAN connections have only begun to grow. As shown in Exhibit IV-9, only a quarter of the agencies surveyed have established LAN-to-WAN connections. Even this data must be viewed with some caution.

The data represents the percent of agencies that have established local-to-wide-area connections, not the number of connections that have been established. Many departments have had need to establish one or more individual connections between local- and wide-area networks, but few, if any, have established connections to wide-area networks for 26% of their local-area networks.

Although the data must be viewed with some caution, it clearly indicates that local-to-wide-area network connections are growing in importance. The high percentage of agencies that plan to have LAN-to-WAN connections in the future indicates the need to have very high wide-area networking capability.

EXHIBIT IV-9



There are several possible reasons for the low percentage today, including a general lack of perceived need and an inability of technology to effectively support these types of connections. INPUT believes there are two primary reasons.

- Agencies recognize that many of their systems need to be enhanced to take advantage of greater user connectivity. Older systems need to be converted to data base systems, and standards and procedures for access and data use need to be established.

- Agencies recognize that networks such as FTS 2000 do not currently support the high bandwidth that will be needed to effectively support integrated, enterprise networks.

Agencies will clearly need assistance in developing enterprise networks. In the short term the primary opportunities are for professional services vendors to assist in developing strategies and migration plans. The data suggests that hardware vendors will need to view the market with a certain amount of patience.

C

Enterprise Networks

As previously noted, a key trend in the development of networks is the evolution toward enterprise networks. Developing an enterprise network is complex and difficult. Integrating local- and wide-area networks necessitates some critical management decisions.

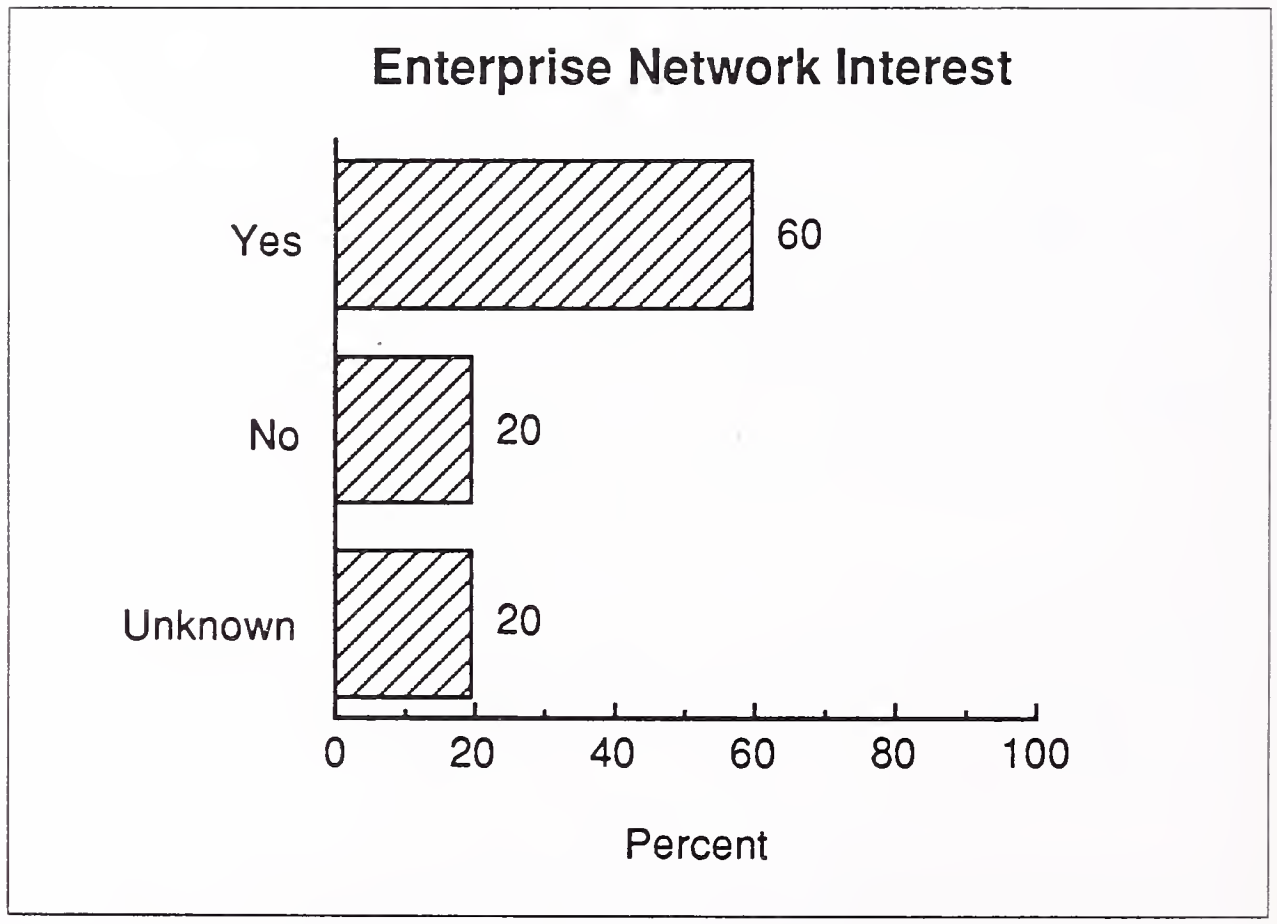
This report seeks to assess interest in developing enterprise networks, identify the types of networks that users believe would best meet their needs, and assess the relationship of network development trends and network management products and practices.

1. Enterprise Network Interest

To assess the interest, users were asked whether their agency had interest in developing an enterprise network. This type of network was generally described as the integration of local- and wide-area networks that would permit any-to-any connectivity both locally and across wide geographic areas such as the country.

Exhibit IV-10 summarizes the results of this query. Agencies are clearly interested in developing networks that support all departments and functions regardless of their geographic location or type of equipment.

EXHIBIT IV-10



Reasons that agencies are not interested are not entirely clear. In one case, a department indicated that it already had an enterprise-wide network. It responded *no*. Another department indicated that it would be interested, but security requirements precluded it from considering that type of network integration. Several agencies indicated that they had not had an opportunity to assess the idea.

The data and supporting comments suggest that actual interest is higher than 60% among organizations that do not currently have extensive networking and are not restricted by regulations or security. INPUT estimates that this figure may be closer to 80-85%.

2. Enterprise Network Types

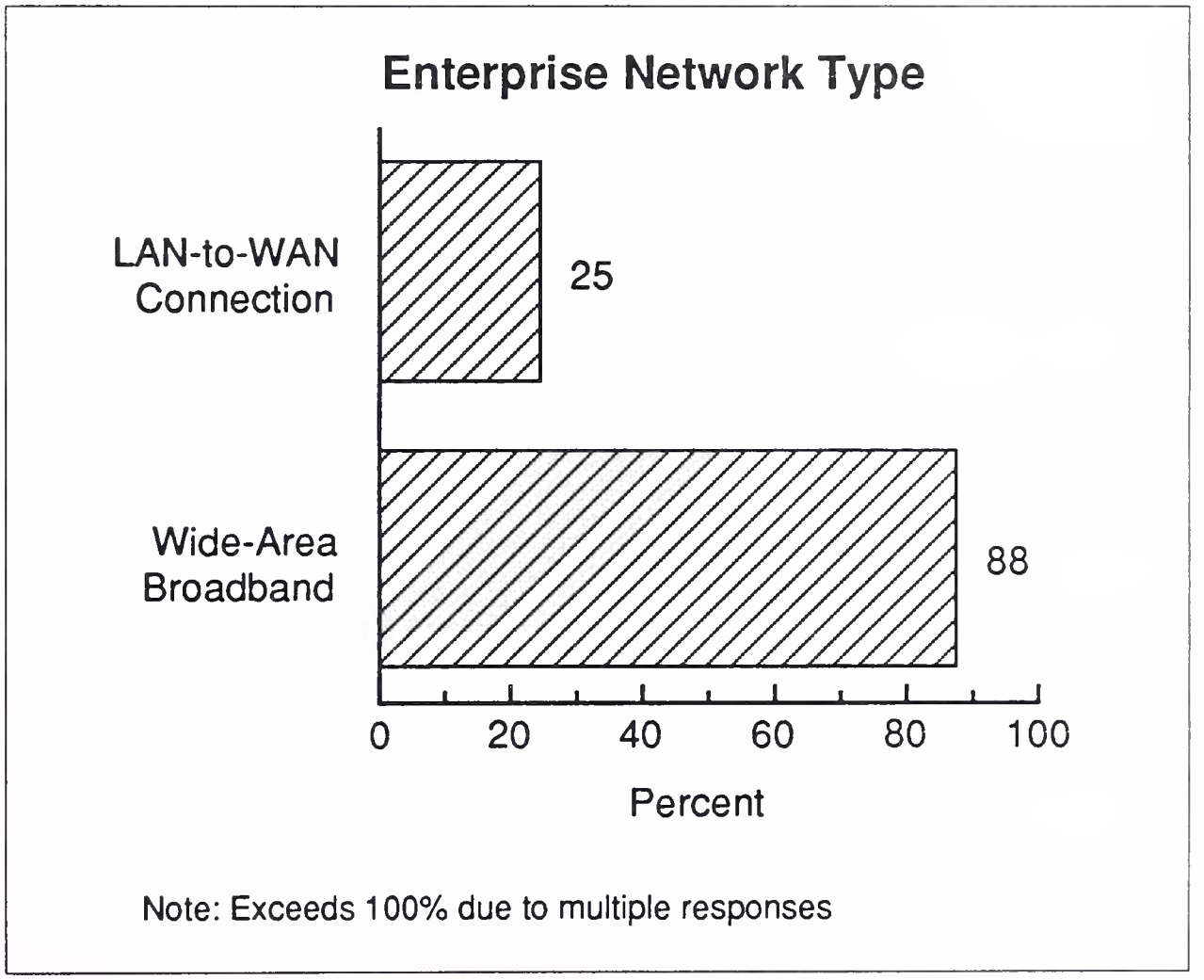
As organizations progress in the development of integrated applications and begin to address organization-wide connectivity, a key question relates to the type of networking that will best meet their needs. There are two basic approaches.

- The first approach is to interconnect LANs within the organization and establish connections between the LANs and traditional (lower speed, wideband) wide-area networks. This is commonly accomplished through the use of routers, etc., today.

- The second approach is to establish high-speed (broadband type) networks that expand beyond the immediate work group or premises.

As can be seen in Exhibit IV-11, agencies clearly believe that they will need to have high-speed networks that cover wide geographic areas.

EXHIBIT IV-11



Note: Exceeds 100% due to multiple responses

Agency interest in wide-area broadband-type networks is consistent with the interest of private sector organizations in the ability to transmit a mix of voice, data, graphics, and video over integrated electronic highways.

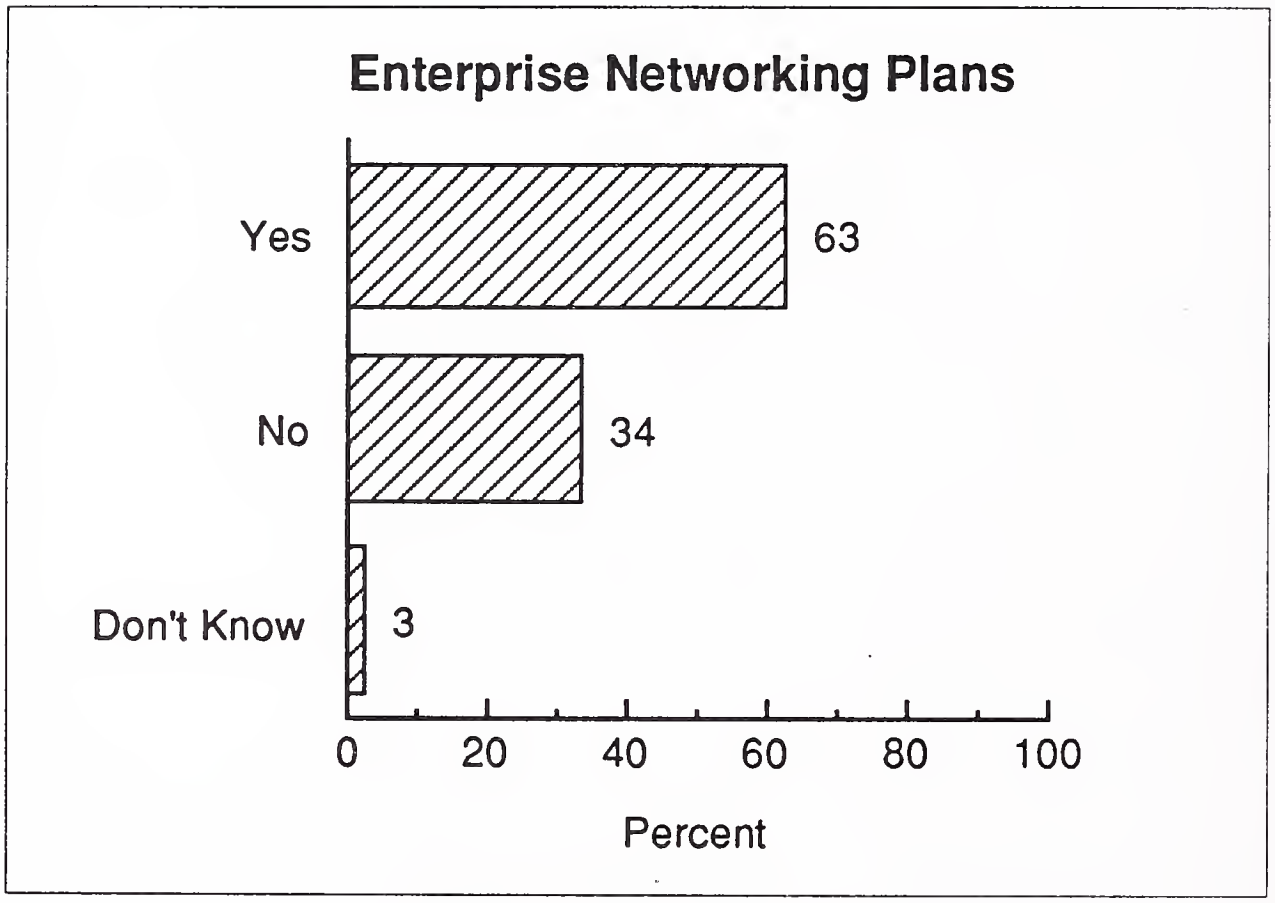
An emerging trend of multimedia transmission adds to the complexity. Interest in multimedia is growing as a means of conducting activities such

as training over wide geographic areas. While exceptionally high-capacity networking (to support activities such as multimedia and image transmission) is needed by only a few organizations today, planning is necessary for organizations to meet future (enterprise) networking requirements.

3. Enterprise Network Plans

As shown in Exhibit IV-12, a high percentage of agencies are currently planning to implement enterprise-wide networks. Sixty-three percent indicate that they either have plans or are in the process of developing plans to implement enterprise networks.

EXHIBIT IV-12

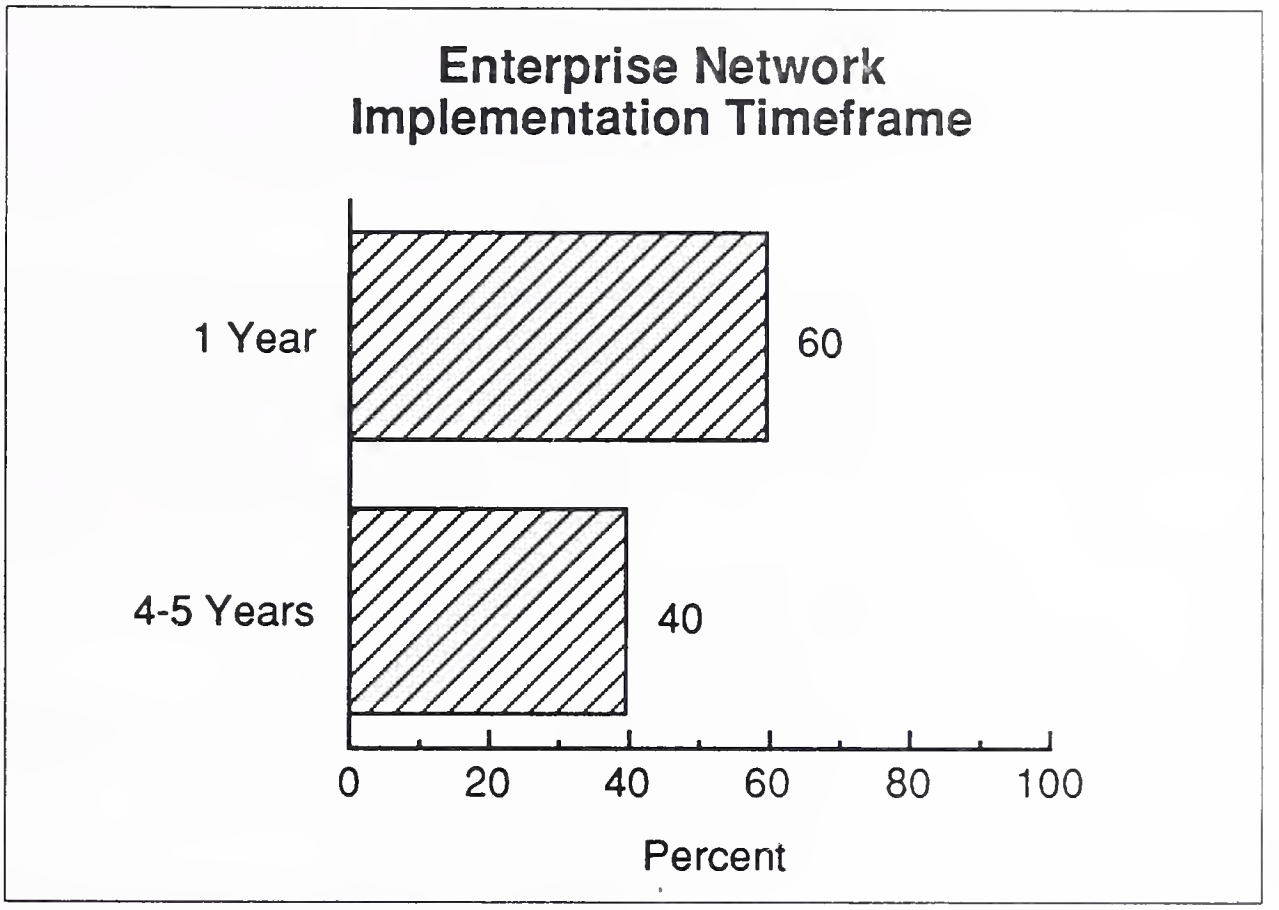


Of the organizations planning to implement enterprise networks, many believe that they will begin to implement the networks within the next couple of years. As shown in Exhibit IV-13, 60% believe that they will begin the implementation process within the next year. All believe that implementation will begin within the next five years.

Although respondents were definitive in their responses, INPUT believes that the extent of planning reported and the timeframes are optimistic.

INPUT believes that many organizations may have, in fact, begun the process of analyzing requirements and may have developed preliminary strategic plans, but there is little to suggest that agencies other than the few largest and most technically oriented are actually ready to begin implementation.

EXHIBIT IV-13



INPUT also believes that a few organizations may begin to implement these types of networks within the next year, but that considerable planning remains to be done before many organizations will be able to begin. And of those that are implemented, the networks may provide little true, any-to-any connectivity, initially.

Telecommunications and IS managers frequently focus, initially, on the technological aspects of networking. They give their attention to analyzing products, product compatibility, and alternatives for establishing physical connections.

Many managers give little attention to the complex management issues of enterprise networking. To illustrate the level of complexity of issues that need to be addressed, consider the following differences between wide-area (typically data) and local-area networks and a number of fundamental questions that must be answered.

D

Federal Network Management

As noted in the previous section, developing and implementing enterprise networks is a highly complex process that goes considerably beyond technological issues. Likewise, managing networks–particularly integrated, enterprise networks–is a complex task. The job will not get any easier, at least in the short term.

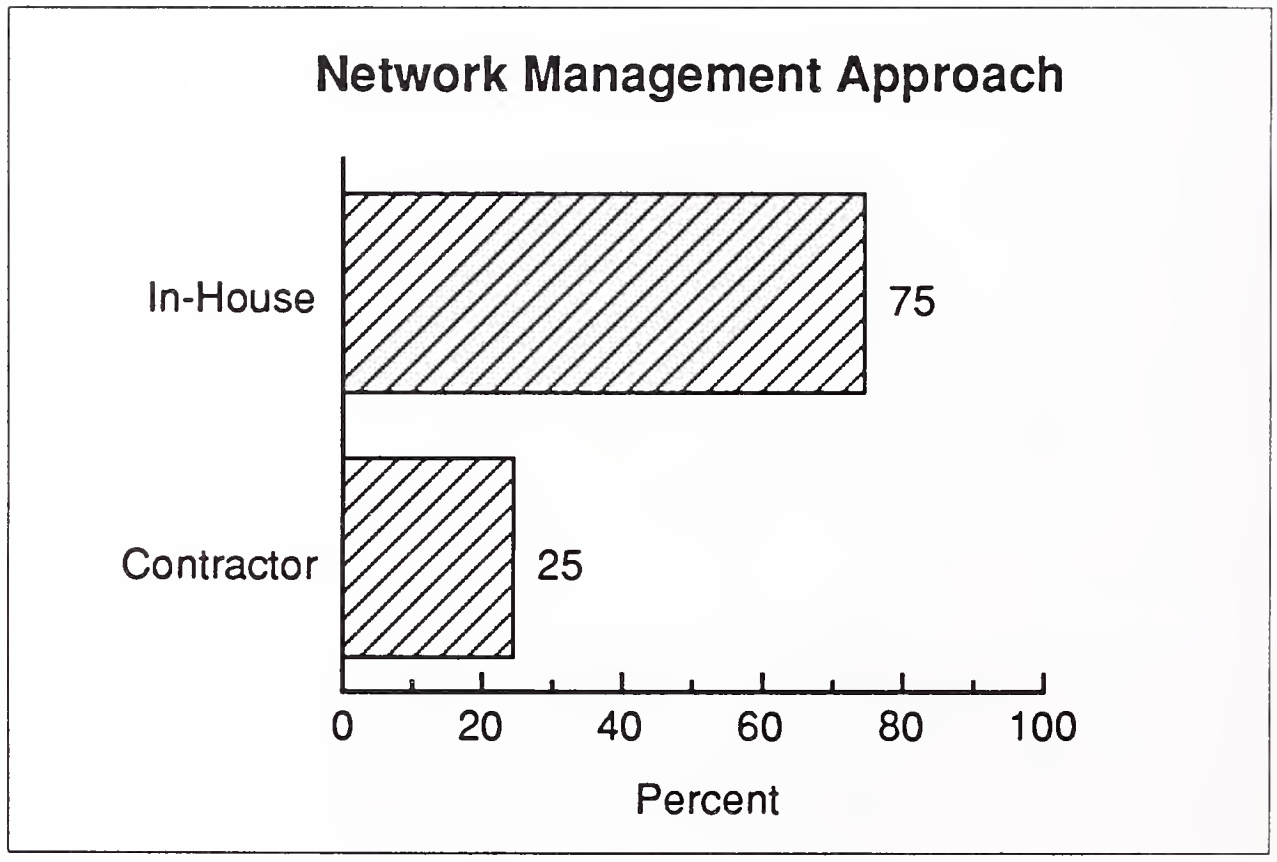
Considerable progress has been made in developing comprehensive network management products over the past two to three years, but much more needs to be done to be able to effectively manage integrated, high-speed, electronic highways that agencies believe they will need in the future.

The following discusses practices related to managing networks in the federal government today. For the purpose of the report, each of the topics was approached from the standpoint of trying to understand how today's processes and practices relate to the governments interest in enterprise networking. This section addresses wide-area networks and local-area networks individually, and then addresses the management of enterprise networks.

1. Wide-Area-Network Management

As indicated in Exhibit IV-14, the majority of federal departments manage their wide-area networks with in-house staff.

EXHIBIT IV-14



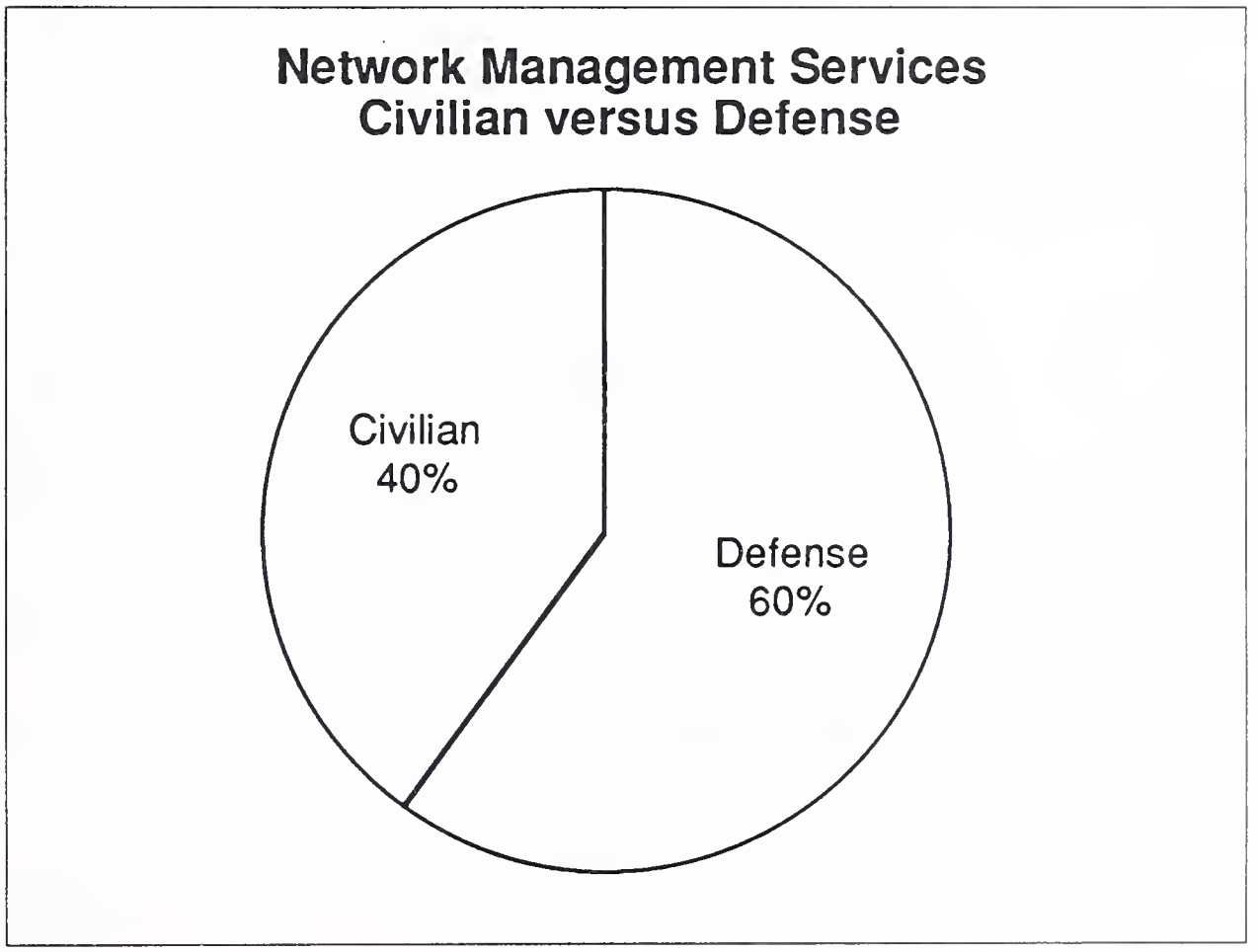
Industry research indicates that, as networks become more complex and critical to day-to-day operations, an increasing number of departments will consider contracting with someone to manage their networks for them.

INPUT believes that this trend will continue and, if the commercial sector can be used as an indication, the 25% could begin to grow to 35-40% over the next several years.

In addition to organizations that have entered into agreements to have their network managed by a contractor, a much greater number of both civilian and defense agencies have contracted for some number of network management services. Typically, these services cover maintenance of local and remote equipment.

As shown in Exhibit IV-15, 60% of expenditures for management services such as maintenance are from the Defense Department. While the Defense Department's expenditures will continue to increase, INPUT expects that, over time, the split between civilian and defense will become closer. At some point, the split could be reversed.

EXHIBIT IV-15

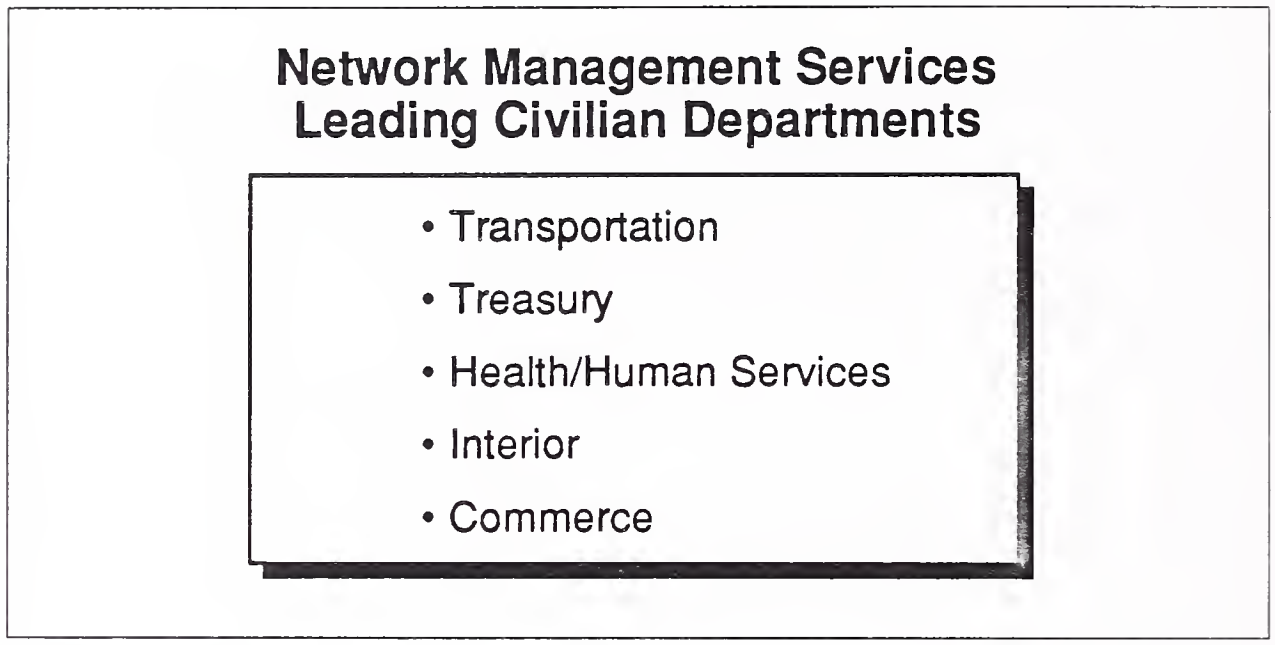


To date, the Defense Department has frequently made greater use of complex networking than have civilian departments. As networking becomes more important and accepted by civilian departments, their proportional share should increase.

Note that the exhibit refers specifically to network 'services.' Network services include a high proportion of maintenance-type service. Maintenance is only one aspect of network management. There is no direct relationship between the percentage of departments that have contracts for a vendor to maintain their networks and those that contract for network management services. Twenty-five percent of agencies surveyed indicated that either a vendor or some other agency manages their network for them. A greater percentage of agencies have contracts for a vendor to provide some type of network (maintenance) service.

Exhibit IV-16 summarizes the leading civilian departments' expenditures for network management services. It's interesting to note that the majority of the leaders in expenditures for network management services are not the leaders in the numbers of wide-area network circuits.

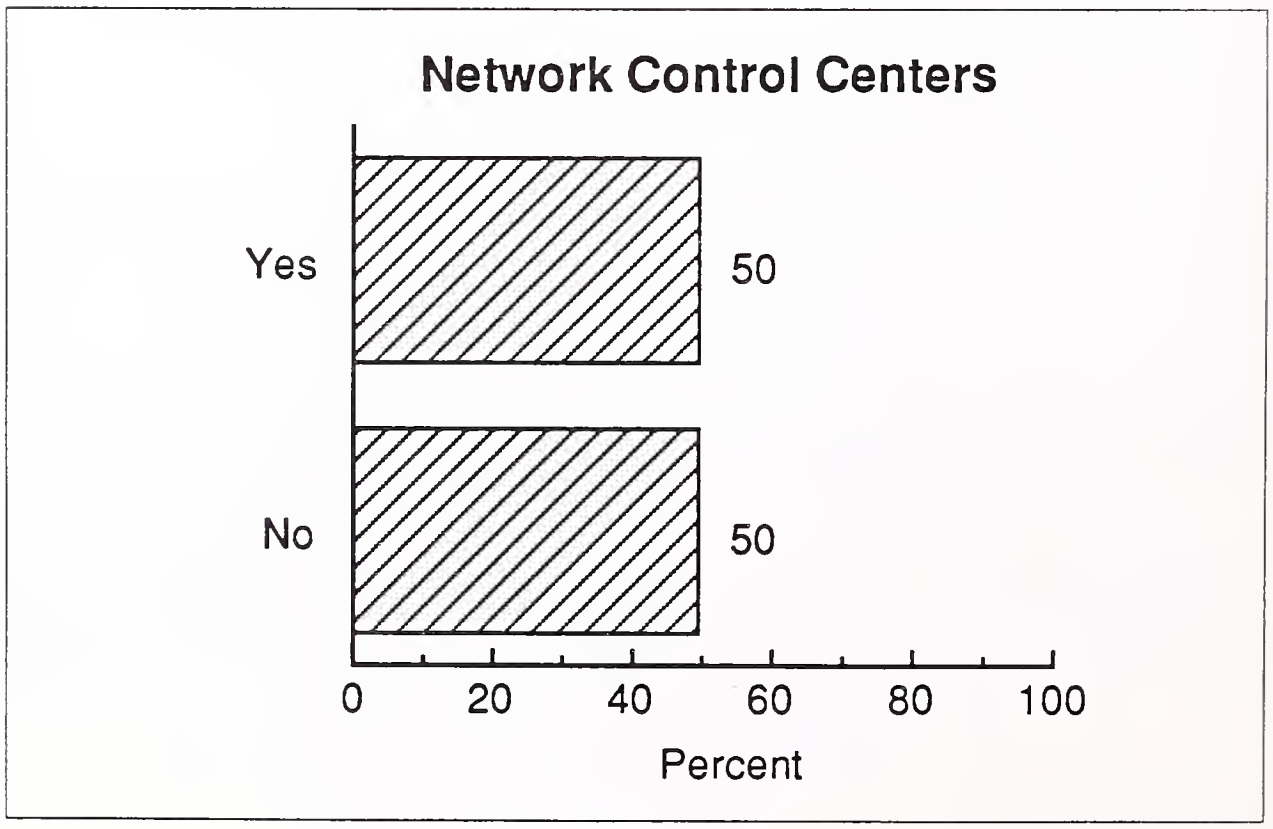
EXHIBIT IV-16



The data suggests that the larger (more sophisticated) the network, the less inclined an organization is to contract for network management services. Conversely, agencies that will be developing sophisticated networks may be more inclined to consider contracting with a vendor.

Recognizing the importance of ensuring effective network management, 50% of federal departments that manage their own networks have established organizations dedicated to managing their wide-area networks, as shown in Exhibit IV-17. However, again the data should be viewed with some caution.

EXHIBIT IV-17



Analysis of responses indicates that, of the leading departments, nearly all have network management centers. The data indicates, further, that few of the smaller departments have organizations dedicated to managing their networks.

For vendors, the differences can be important. While the large departments would generally represent the greatest revenue opportunities, the smaller departments are frequently the ones that have the greatest need. The data suggests that vendors may need to devote a greater portion of their effort to assist the somewhat smaller departments that need assistance.

Of the departments that manage their own networks, there is no single preferred approach to managing wide-area networks. Data from federal departments is generally in line with the data from the private sector. Exhibit IV-18 identifies the frequently mentioned approaches to managing wide-area networks. The approaches are not in order of importance.

EXHIBIT IV-18

Wide-Area Network Management Approach

- Netview
- Modem control systems
- TI control systems
- Other

The most frequently mentioned approach to managing networks is *other*. The *other* category accounted for 43% of the responses. Netview was second with 29% of the responses. The percentage is particularly important when considering requirements for the future.

A similar situation would be found in the private sector. The majority of organizations have not yet settled on the best product or approach for managing wide-area networks. In addition, many organizations have been reluctant to make major investments in network management products and services.

The majority of organizations use a variety of products to perform technical analysis of circuits, but are just beginning to implement comprehensive, integrated network management systems. Federal departments are not any different. They recognize the need, but have, as yet, not been prepared to make major investments. There are two primary reasons.

- Networking standards have not stabilized. There is still too wide a variety of products with proprietary features. Departments are reluctant to make investments in management products that will not be able to interact with installed equipment.

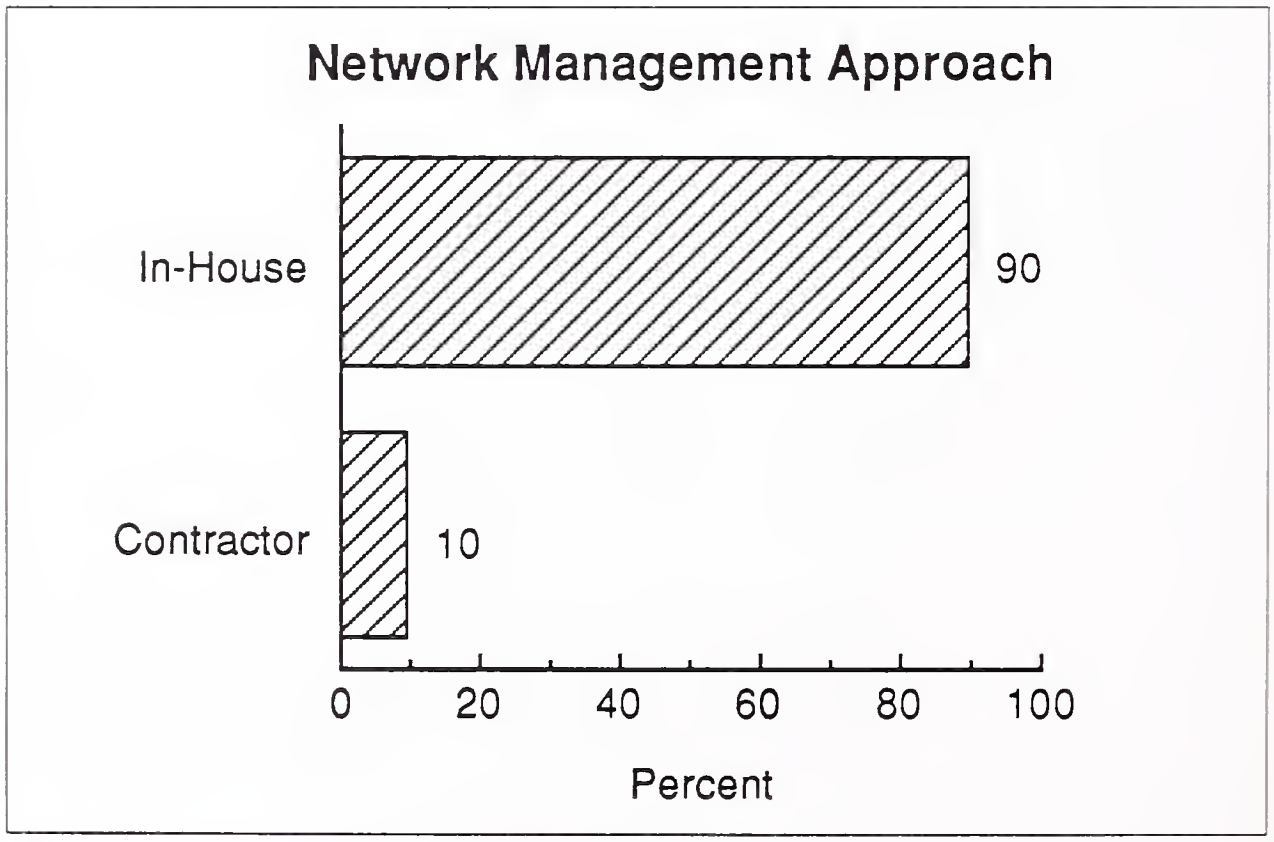
- Network management products are still weak. Significant progress has been made, but many network management products are able to interact with only a few types of computing and terminal equipment.

The low percentage of responses for modem- and multiplexer-based network management systems is found in both the private and public sectors. Users believe that products must be considerably more comprehensive than those a single modem or multiplexer hardware manufacturer is able to provide.

2. Local-Area-Network Management

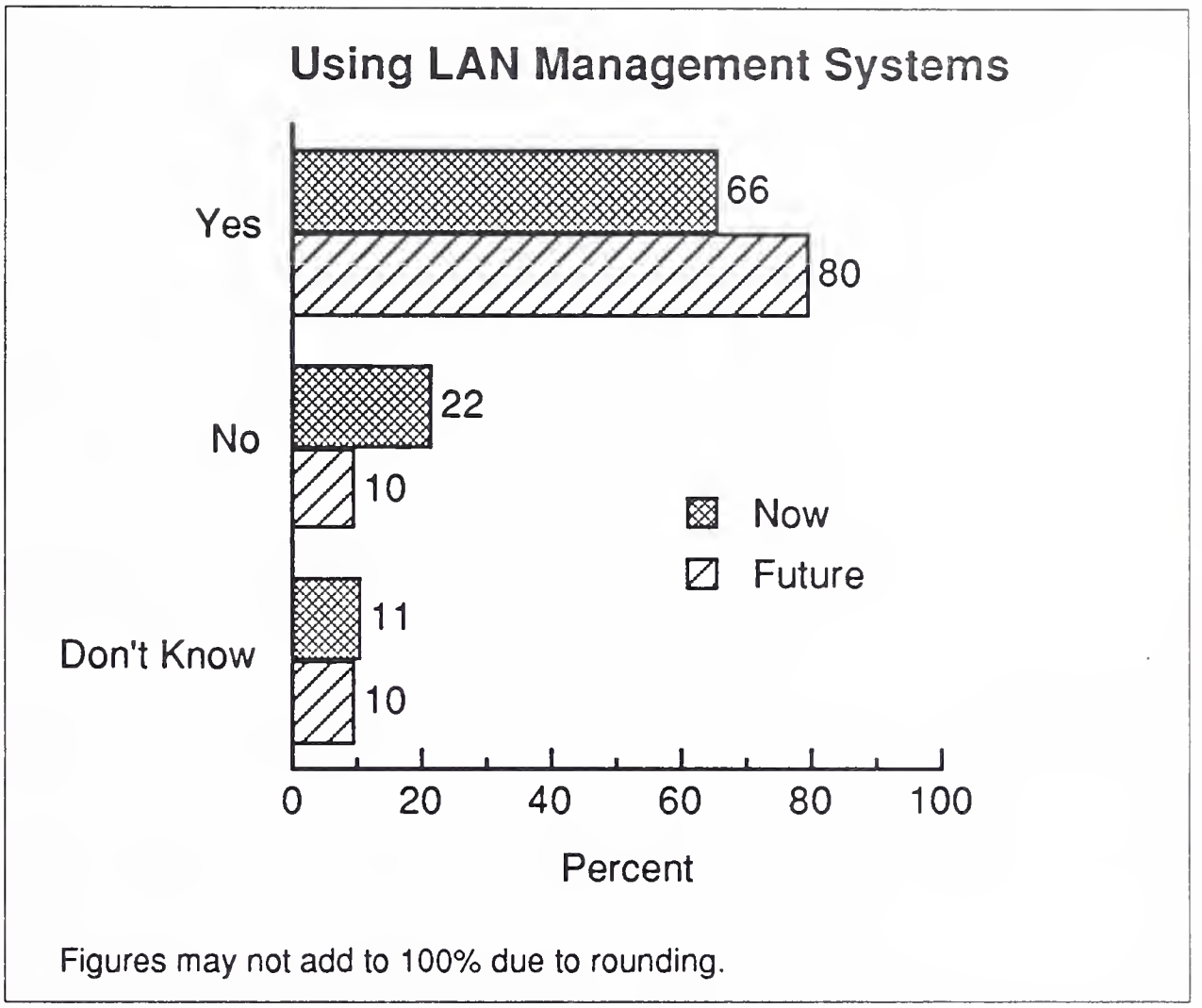
As shown in Exhibit IV-19, the percentage of local-area networks managed by in-house staff is considerably higher than for wide-area networks (90% vs. 75%). This is not expected to change in the short term, but could begin to change as local-area networks begin to look more like wide-area networks.

EXHIBIT IV-19



The percent of departments indicating that they use some type of LAN management system attests to the growing importance of LANs. Equally clearly, LAN management systems will be an operating necessity within the next few years, as shown in Exhibit IV-20.

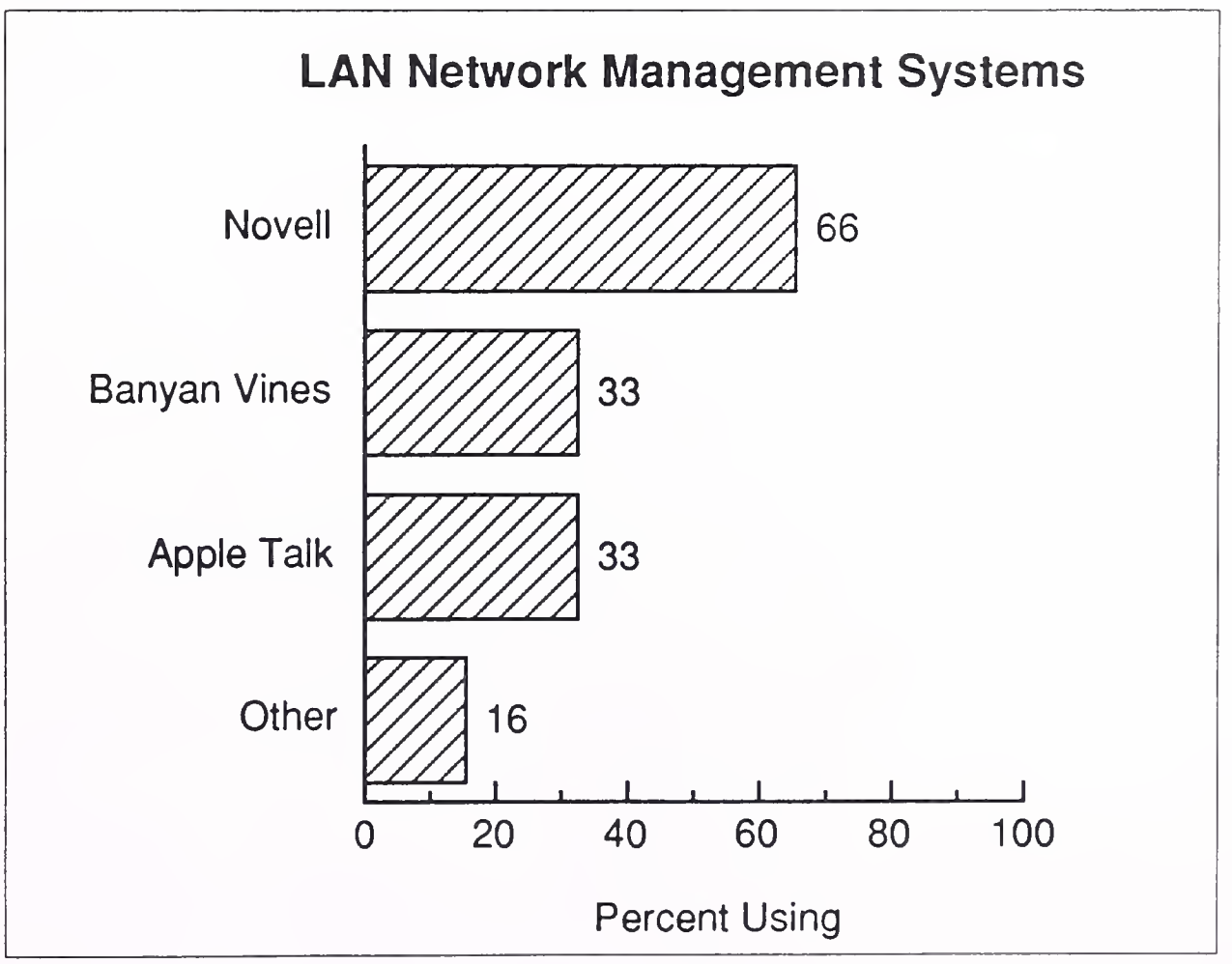
EXHIBIT IV-20



Figures may not add to 100% due to rounding.

The most frequently mentioned LAN management systems are shown in Exhibit IV-21. From the data, Novell is clearly the preferred choice.

EXHIBIT IV-21

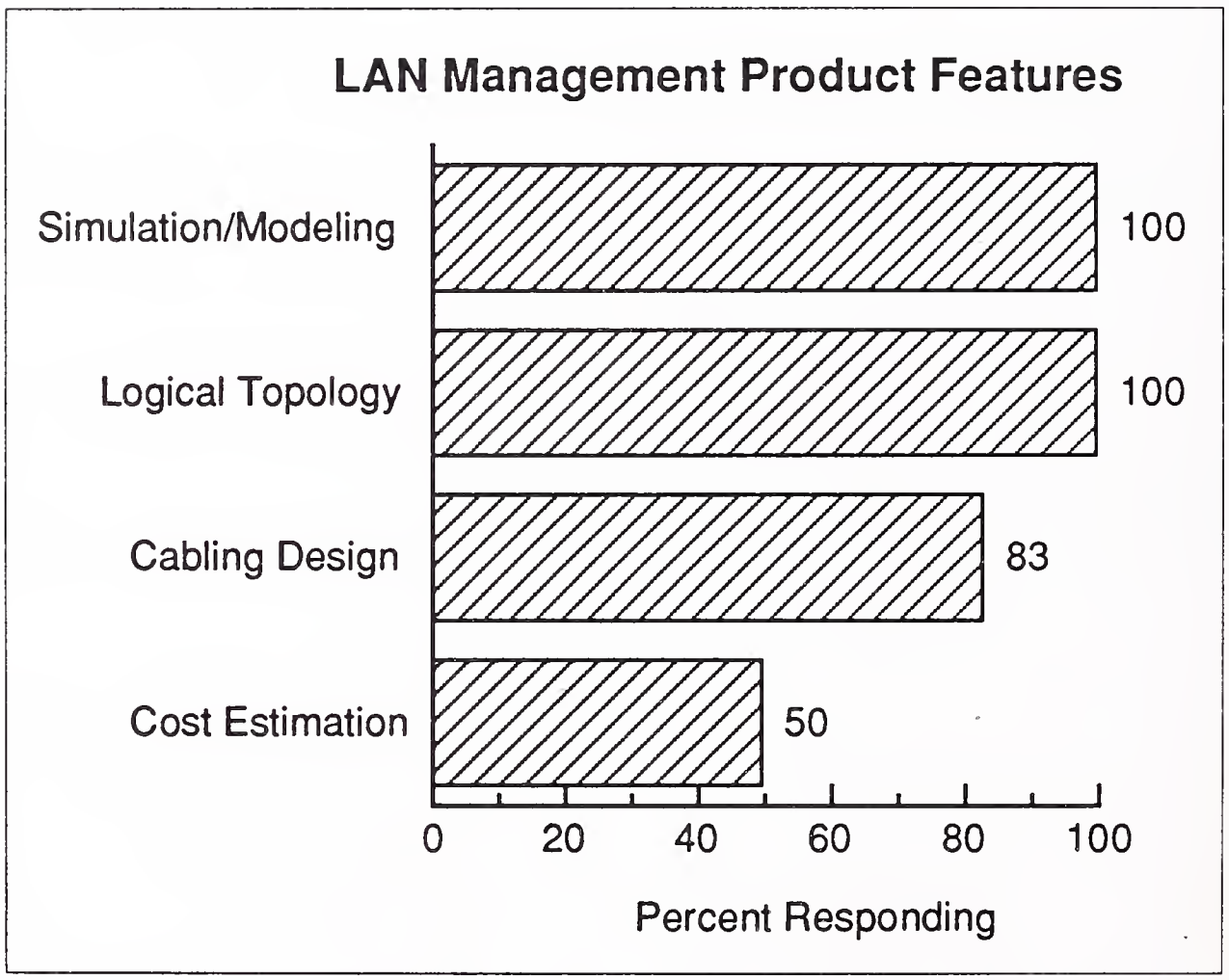


It is interesting to note that AppleTalk was mentioned as a network management tool by a third of the respondents, since few respondents made specific reference to networks for Apple computers. There are numerous Apple (particularly Macintosh) systems in the federal government, but few respondents made specific reference to them.

As part of the research, INPUT sought to identify features that users believe are important in LAN management products. Note that INPUT assumed that users will want integrated products that permit analysis of all types of devices on a network. User comments supported the assumption. The questions were focused on the types of features that will provide added value.

As shown in Exhibit IV-22, simulation/modeling and an ability to analyze logical topology were mentioned as important by all respondents.

EXHIBIT IV-22



Simulation and modeling will become increasingly important as high-speed (LAN) networks become more common and users want to attach a greater number of devices. Network managers must be able to perform analysis of the impact of adding additional devices to a network. Inclusion of logical topology is understandable. It is also indicative of a problem that will grow in importance.

The high percentage of responses indicating *unknown* or *other* to questions about the types of LANs installed suggests that maintaining a comprehensive network profile will be difficult. Managers of wide-area networks know from experience that understanding both physical and logical topology is vital to effective network management.

For network managers to successfully manage a network, particularly a local-area network, they must have knowledge of all components on a network and the type of data transmitted to and from each.

3. Integrated Network Management Product Needs

Managing an integrated (enterprise) network is complex. Recognizing the complexity, users were asked to identify major needs for successfully managing integrated networks.

Federal departments believe that the greatest need, to be able to successfully manage integrated networks, is for standards, as shown in Exhibit IV-23. The same concerns are found in the private sector, as are the other identified needs.

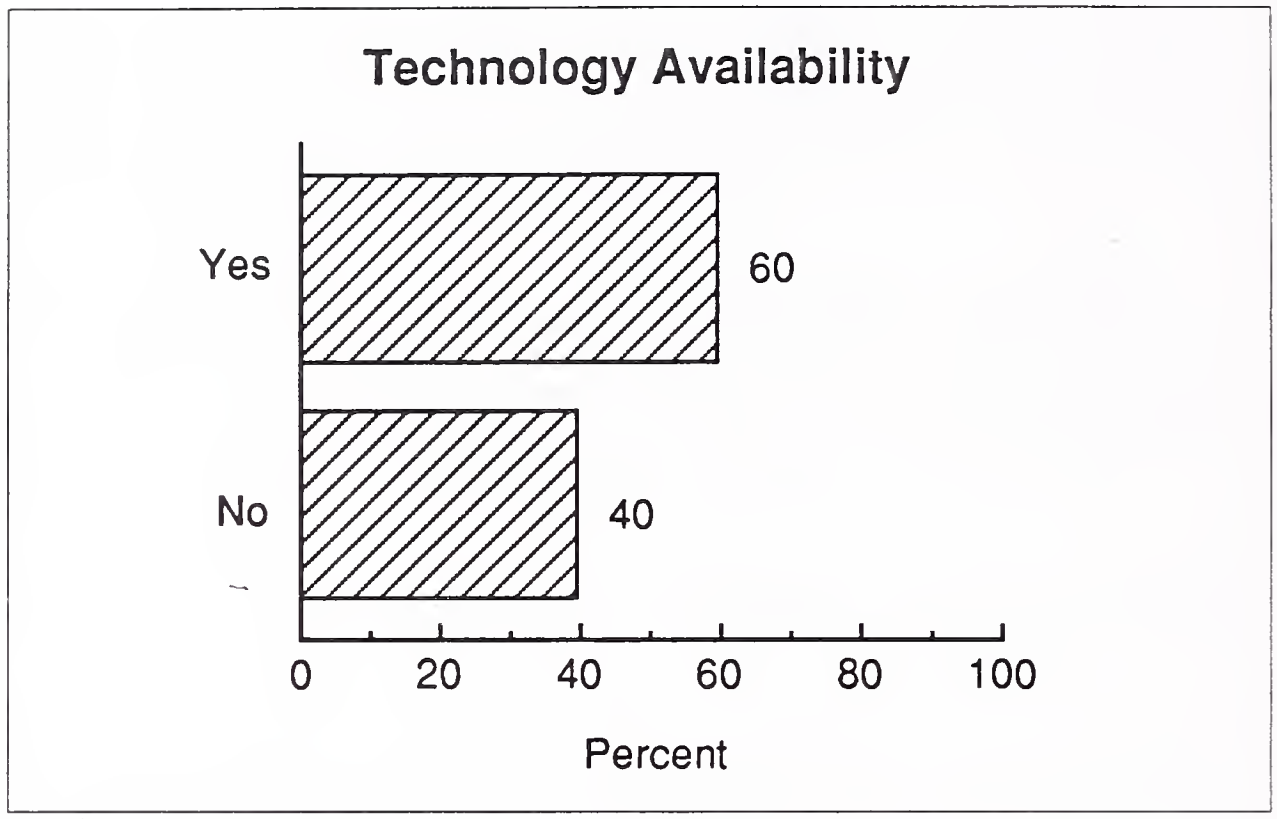
EXHIBIT IV-23

Enterprise Network Management Needs

- Standards
- Integrated management tools
- Management commitment
- Consistent network structure

While the needs identified were not surprising, the percentage of respondents indicating that technology is available today to successfully manage integrated networks was unexpected. As shown in Exhibit IV-24, 60% of users believe that technology is available today to successfully manage integrated (local- and wide-area) networks. Private sector responses would generally be the reverse.

EXHIBIT IV-24



The reasons for the difference between federal and private sector responses are unclear. There are at least a couple of possible explanations.

- Network management products have improved significantly over just the past couple of years. Compared to what managers have had to work with in the past, the products are a dramatic improvement. Federal network managers may be reflecting interest in the enhanced (current) capabilities, rather than an actual belief that the products will meet future needs.

- Many managers may be focused on somewhat narrow technical issues. Organizations whose network(s) are predominantly single-vendor networks may, in fact, be able to obtain the needed network management products.

INPUT believes that the issues are somewhat more complex.

- Many agencies have yet to address the complex issues of integrating office systems, the predominant use for LANs, and application systems. As noted previously, there are numerous technical, functional, and management considerations.

- Many agencies have a high expectation that they will be able to obtain network management services as a by-product of using FTS 2000.

- Few agencies have begun to give specific consideration to integrating and managing the wide variety of terminals, workstations, PCs, and computers currently installed.

These points are not to suggest a specific lack of focus on the part of federal organizations. The same situation is found in many private sector organizations. The points are to suggest that most organizations are still focused on meeting short-term needs for local connectivity.

4. SNMP or CMIP

As with the evolution of network architectures as a whole, the prospect for comprehensive, standard network management products is cloudy. There are numerous products available to manage local-area networks. Product quality ranges from high to extremely low. A key characteristic of many products is that they provide diagnostic and management capability for a specifically defined set of networking equipment. The equipment is frequently the vendor's equipment.

While the list has been growing, there are few products that are totally vendor independent and fewer yet that can manage the wide variety of equipment found in federal networks. Because of the need to manage this wide variety of equipment, industry has been working to develop standards for network management products. The two leading contenders for standard, industry-wide products are SNMP (Simple Network Management Protocol) and CMIP (Common Management Information Protocol).

SNMP is based on TCP/IP protocol standards. As the name implies, it is intended to be simple. However, its simplicity is the root of its difficulty. SNMP does not run on non-TCP/IP token ring networks and it does not provide support for Ethernet networks supporting DECnet routers. TCP/IP and DEC are both prominent in federal networks. Tests of SNMP have also indicated that it can consume as much as 10% of a network's bandwidth to operate.

In contrast to SNMP, CMIP (Common Management Information Protocol) is based on OSI protocol. CMIP standards are much more comprehensive, but have not been finalized.

There are currently an estimated 100 SNMP-based products. There are no viable CMIP products available. CMIP products are beginning to emerge, but there are few available and users are uncertain whether they will actually work with the wide variety of protocols currently installed. An acceptable set of CMIP products is not expected for at least the next year or two.

The federal government has indicated that it will support CMIP. CMIP is consistent with the government's support of GOSIP and appears to offer much richer network management capabilities for the future.

Recognizing that network management product standards are important, the government has prepared the Government Network Management Profile (GNMP). The intent is to provide a profile of standards that the

government will support in its buying policies. The focus of the profile is on OSI, TCP/IP, and FDDI.

Review and acceptance of a federal network management standard is expected to require from one to three years. Comments are currently being made on the proposed profile, with revisions expected at a later date.

Few, if any, agencies have made specific commitments to either set of standards. However, there are indications that SNMP may be satisfactory as a short-term solution. As one example, the Air Force will use SNMP in many of its TCP/IP over Ethernet integration projects. This will apply to its ULANA project.

In one set of industry research, more than half of the organizations surveyed indicated that they would continue to consider SNMP a viable network management product for the next 3 to 5 years. In the same survey, a third said that they have no specific plans for CMIP products.

In the meantime, organizations such as the EPA are beginning to finalize basic networking strategies. The EPA has already begun to re-allocate some of its information systems funds away from mainframe computing to develop networks based on products that provide interoperability. It has chosen a Novell (network) operating system, token ring architecture, and IBM's LAN Manager as the network management tool.

In the short term, INPUT expects that most agencies will take the same general approach that the EPA is taking.

- They will focus on interoperability.
- They will select products that will be able to work with the SNMP. To the extent possible, they will try to provide for conversion to CMIP, but this is of secondary importance.
- They will select network management tools that enhance their ability to manage the growing number of LANs better.
- They will wait for standards to evolve.

INPUT believes that some time will be required for agencies to begin to address comprehensive enterprise networking. By the time they are ready to implement enterprise networking architecture, the standards picture will be somewhat more clear. Most agencies will adopt a wait-and-see perspective.

5. Network Management and FTS 2000

As discussed in INPUT's *Federal Telecommunications* report and in earlier sections of this report, many organizations have been waiting for FTS 2000 to become a reality before initiating changes to their networks. Many agencies had placed networking projects on hold until the FTS 2000 contract was finalized. The network is now a reality and questions have been raised about the ability of FTS 2000 to provide comprehensive (data) networking capability.

INPUT believes that FTS 2000 will be able to meet the majority of agency wide-area networking needs, but questions whether FTS 2000 will be able to support either the very high bandwidth necessary for broadband enterprise networks or to provide comprehensive, integrated, enterprise-wide network management products.

To a great extent, FTS 2000 is caught in a Catch 22 situation. The network was developed to provide inter-exchange network services, not local-area services. Neither Sprint nor AT&T can provide true, end-to-end connectivity. Also, local-area networking services are not part of the offerings.

Agencies wanting to develop and manage enterprise (local- and wide-area) networks are faced with a need to manage a network comprised of local-area networks, a metropolitan-area network, and a wide-area network. Since FTS 2000 only addresses wide-area needs, agencies are uncertain how to proceed to meet other needs. More importantly, they are uncertain about who will be able to provide end-to-end enterprise networking.

Because of the need to interact with multiple vendors providing different levels of network products, services, and expertise, INPUT believes that FTS 2000 cannot be looked at as a viable source of management service for all of an agency's network management needs.

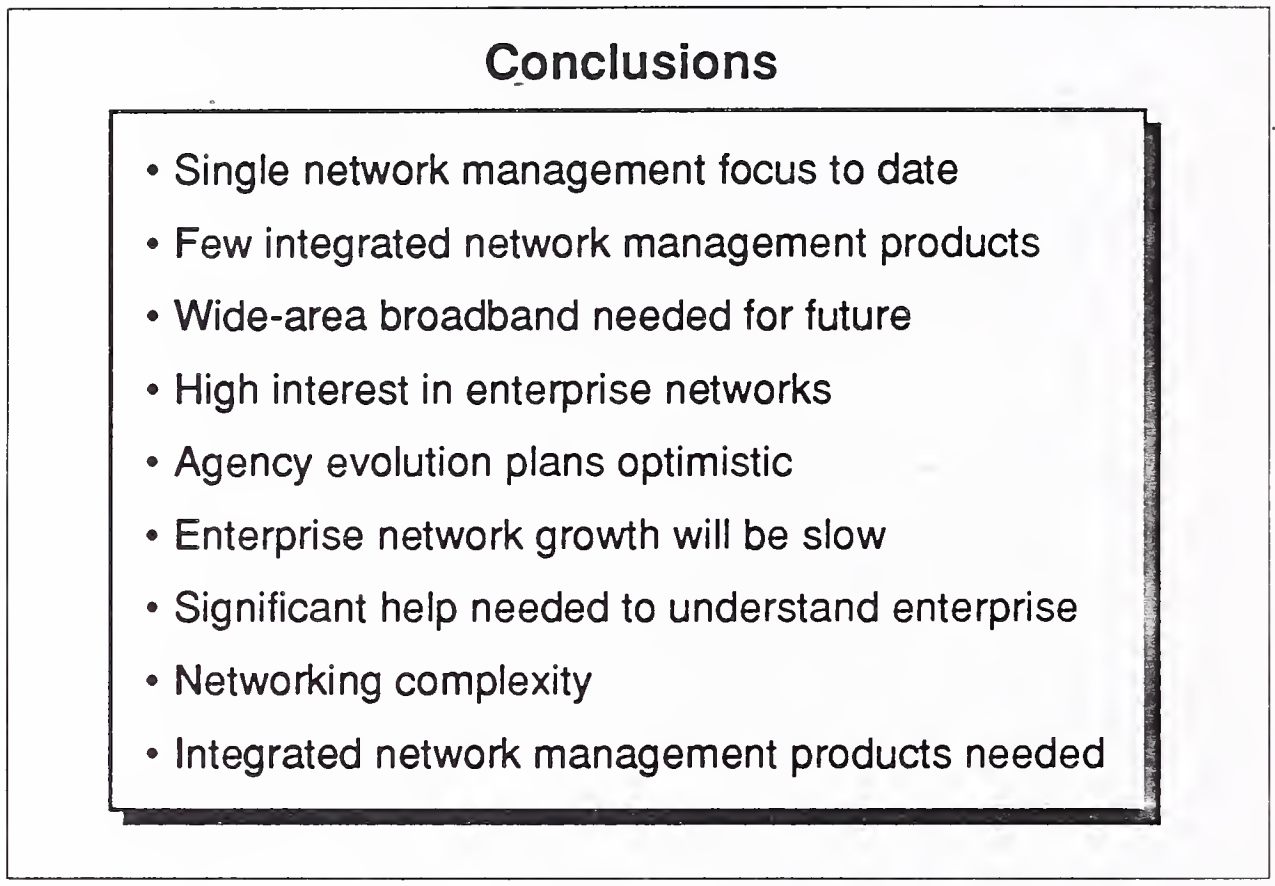
As networks become more integrated and complex, agencies will need to identify methods to manage the wide variety of networks, network components and network vendors. They will need to either develop in-house expertise, contract with another federal agency, or turn to an outside vendor to provide network management services.

E
Conclusions and Recommendations

There are numerous conclusions and recommendations that can be drawn from the data. Many of the conclusions relate to the current (technological) state of networking in departments throughout the federal government.

There are an equal number that relate to management needs to migrate to enterprise networking. Exhibit IV-25 provides a summary of major conclusions.

EXHIBIT IV-25



Overall, the network management environment in the federal government is not significantly different than in the private sector. Isolated networks have evolved to meet specific applications needs. Network management products and processes have been implemented to manage individual networks. As with the private sector, this is beginning to change.

Acting as electronic highways, networks of the future will need to provide bandwidth orders of magnitude higher than today. They will provide the means to transmit a wide variety of data concurrently. In high-capacity networks, much of the data volume and flow will be unpredictable.

To meet the needs of the future, network management processes will be more analogous to managing the flow of automobiles at the intersection of four six-lane interstate highways at rush hour than managing the data on several data circuits. Network management products and services will need to reflect the change. Development of enterprise networks will be an evolutionary process. For vendors focusing on short-term market opportunities, the process might be viewed as excessively slow.

The following recommendations are provided to help vendors of network management products and services realize maximum opportunity from a young market and establish positions so as to be prepared for future market growth. Key recommendations are shown in Exhibit IV-26.

EXHIBIT IV-26

Recommendations

- Educate users
- Focus on network planning
- Establish system/network vendor alliances
- Develop integrated network management solutions

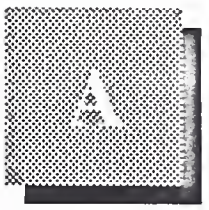
- There is a significant need to educate end users in both the benefits and problems of enterprise networking. Many users tend to view enterprise networking as an extension of establishing connections between several PCs and a printer.

- The major short-term need is to provide an architectural approach from which to grow. Strategic approaches need to be established before real interconnectivity can progress. Without an architecture strategy, many could end up with piecemeal implementation that could be a management nightmare.

- Vendors of network management products and services need to establish alliances with hardware providers both to ensure a presence and to ensure an understanding of solutions that are possible. Without alliances, service vendors may lack technical knowledge of connectivity options.

- There is a particular need for integrated network management solutions. This need is not expected to abate until hardware vendors accept that interconnectivity is of greater value to users than vendor-specific protocols, no matter how much better the vendor's approach may be.

The market for integrated network management solutions is still young. Several years may be needed for the market to begin to mature. Successful vendors will establish early relationships through consulting and education and be prepared to respond to specific product/service needs as they develop.



Federal Network Management User Questionnaire

1. Do you have some knowledge and understanding of the data processing networking systems in your agency?
   _____ Yes
   _____ No (If No, who might we contact?)

   _____

Wide-Area Networks

2. What kinds of host computers, and approximately how many units do you use to support your wide-area network(s)? (Please mark all that apply.)

	Host Computer	Quantity
IBM	_____	_____
Unisys	_____	_____
Digital	_____	_____
Honeywell	_____	_____
Other (please specify)		
_____	_____	_____
_____	_____	_____
_____	_____	_____

3. How many terminals are connected to a host in each of the following manners?

   _____ Locally
   _____ Remotely
   _____ Both

4. For the following connection methods, please state whether local or remote terminals are connected in this manner.

	Local	Remote
Agency-Specific Dedicated Network	_____	_____
FTS/FTS 2000	_____	_____
Dial-Up	_____	_____
Value-Added Network (Not FTS)	_____	_____
Local-Area Network	_____	_____
Other (Specify)	_____	_____
Don't Know	_____	_____

5. Was there a specific reason why you have chosen the method of connection that you are using? If yes, what was it?

_____

_____

_____

6. For the following connection methods, please state whether local or remote terminals will be connected in this manner **five years from now.**

	Local	Remote
Agency-Specific Dedicated Network	_____	_____
FTS/FTS 2000	_____	_____
Dial-Up	_____	_____
Local-Area Network	_____	_____
Value-Added Network (Not FTS)	_____	_____
Other (Specify) _____	_____	_____
Don't Know		

7. Is your wide-area network managed by:
   _____ In-house staff
   _____ Contractor-provided service (Who?) _____
   _____ Other government agency (Who?) _____

8. What kind of network control center is used and what vendor(s) supply these? (If more than one, please mark all that apply.)

	Vendor
IBM Netview	_____
Modem Control Systems	_____
T1 Control Systems	_____
Other (Please Specify) _____	

9. Rate the importance of each of the following network management features on a scale of 1-5 (1 = Not important, 5 = Very high importance)

Single-terminal control of entire integrated network _____

Graphics display of network configuration status _____

Expert system diagnostic tools _____

Natural language user interface _____

Network management utilities, such as service order processing, trouble processing, or inventory control _____

Other features (Please specify)

_____

Local-Area Networks

10. Do you have any LANs in your organization?

_____ Yes
No

11. What percentage of your organization's LANs are connected to **more than one** other LAN today?

_____%
_____ None
_____ Other (Please specify) _____

12. What percentage of your organization's LANs will be connected to **more than one** other LAN five years from now?

_____%
_____ None
_____ Other (Please specify) _____

13. What percentage of your organization's LANs are connected to a wide-area network today?

_____%
_____ None
_____ Other (Please Specify)_____

14. What percentage of your organization's LANs will be connected to a wide-area network five years from now?

_____%
_____ None
_____ Other (Please specify) _____

15. **If None to previous question** - Do you plan to connect one or more LANs to wide-area networks within the next five years?
_____ Yes
_____ No

16. Who manages your LANs?
_____ In-house staff
_____ Contractor (Who?) _____
_____ Nobody
_____ Other (Please specify) _____

17. Are you (or the contractor), using network management on your LAN?
_____ Yes
_____ No (Go to 20)
_____ Don't Know

18. What network management products are used (Check all that apply)?
_____ Banyan Vines
_____ DEC PCSA
_____ Novell Netware
_____ Sitka TOPS
_____ AppleTalk/Apple Share
_____ Other (Specify) _____
Don't know

19. What type of computer manages your LAN?
_____ PC on the LAN
_____ Minicomputer
_____ Mainframe

20. Do you plan to use network management on your LAN?
_____ Yes
_____ No
_____ Don't know

21. What are the characteristics of your LANs? Please indicate how many of your LANs conform to each appropriate LAN characteristic.

	Number
Ethernet	_____
Token Bus	_____
Token Ring	_____
Don't know	_____
Other (Please specify)	

_____

22. Do you have a requirement for a LAN design tool?
_____ Yes
_____ No

23. **If yes,** what features should be incorporated? (Please mark all that apply)

_____ Modeling and Simulation
_____ Logical Topology
_____ Physical Cabling Design
_____ Cost Estimate Modeling
_____ Other (Please specify)

_____
_____

24. Please identify the three leading criteria for selecting a local-area network management system.

_____
_____
_____

Network Planning

25. Does your agency have an interest in developing an enterprise-wide network?
_____ Yes
_____ No **(Go to 28)**
_____ Other (Please specify) _____

Interviewer Note: An enterprise-wide network is a network that has the ability to connect all voice and data services at all locations through a single network. The network can also accommodate video, if needed. For an agency that has little need to connect remote offices, a network that connects headquarters offices and departments would qualify.

26. Which of the following would best represent your thinking of the best way to develop an enterprise-wide network?

_____ Wide-area network with individual LANs connected as necessary
_____ Agency-wide, high-speed (LAN) network that would accommodate voice, data, and image
_____ Other (Please describe briefly)
_____
_____

27. Do you have any specific plans to develop an enterprise-wide network?
_____ Yes (Go to 29)
_____ No

28. Assuming the availability of funds, what are the top three reasons why you do not have plans to develop an enterprise-wide network?

_____
_____
_____

Go to 31

29. Assuming the availability of funds, when would plan to begin implementing an enterprise-wide network?
_____ 1 Year
_____ 2-3 Years
_____ 4-5 Years
_____ Over 5 years

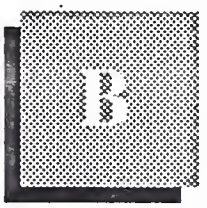
30. Please describe what is necessary to successfully manage the operation of an integrated, enterprise-wide network?

_____
_____
_____

One additional question

31. Do you think that the technology is available to successfully develop and manage an enterprise-wide local-area network?
_____ Yes (Go to end)
_____ No (Why not ?)_____
_____
_____

Thank you for your help



Definitions

The definitions in this appendix include hardware, software, services, and telecommunications categories to accommodate the range of information systems and services programs described in this report.

Alternate service mode terminology employed by the federal government in its procurement process is defined along with INPUT's regular terms of reference, as shown in Exhibit B-1.

The federal government's unique, nontechnical terminology, associated with applications, documentation, budgets, authorization, and the procurement/acquisition process, is included in Appendix C, Glossary of Federal Acronyms.

A

Delivery Modes

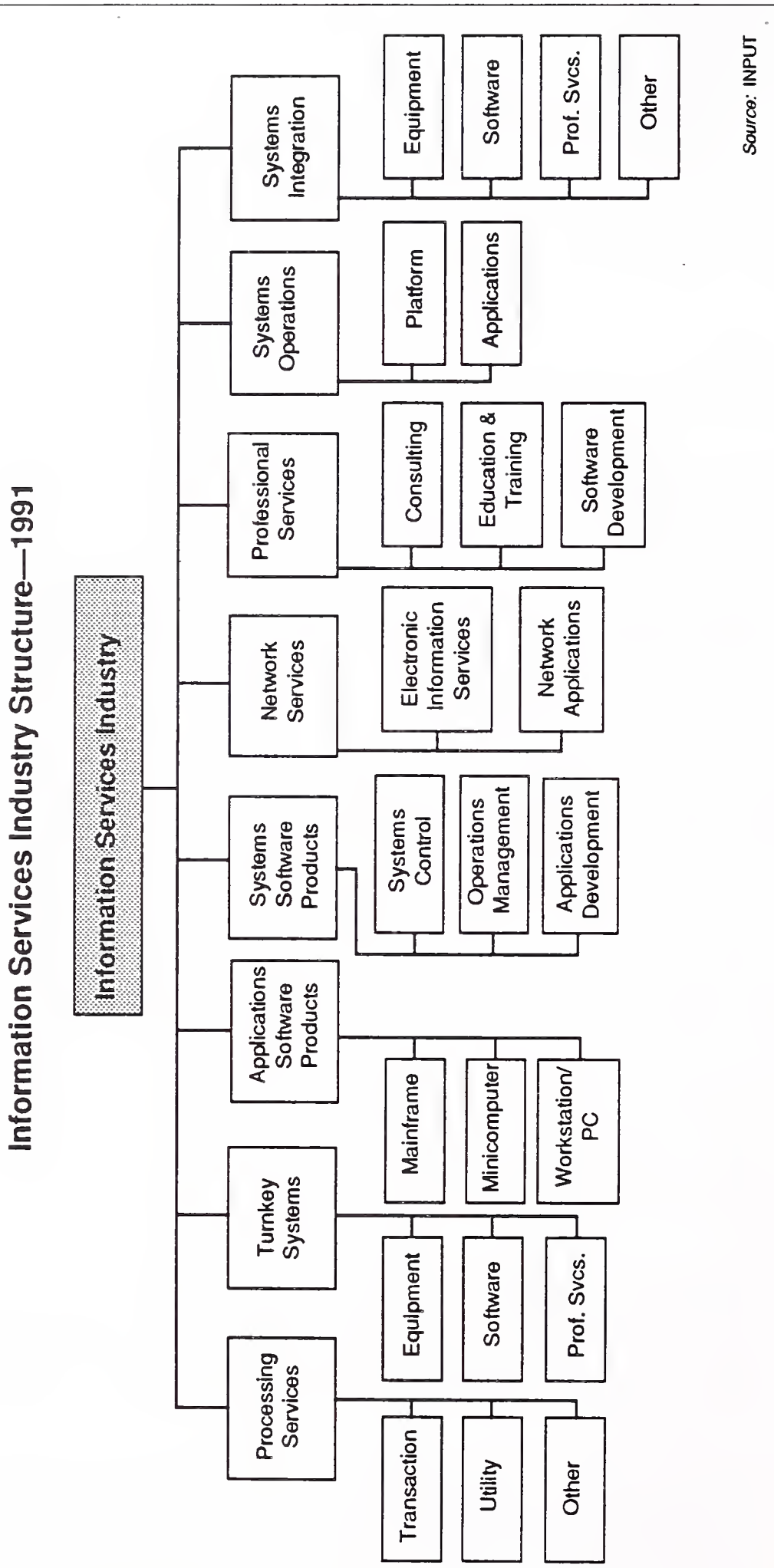
Processing services - This category includes transaction processing, utility processing, other processing services, and processing facilities management.

- *Transaction Processing Services* - Updates client-owned data files by entry of specific business activity, such as sales order, inventory receipt, cash disbursement, etc. Transactions may be entered in one of these modes:

  - *Interactive* - Characterized by the interaction of the user with the system, primarily for problem-solving timesharing, but also for data entry and transaction processing; the user is on-line to the program files. Computer response is usually measured in seconds or fractions of a second.

  - *Remote Batch* - The user hands over control of a job to the vendor's computer, which schedules job execution according to priorities and resource requirements. Computer response is measured in minutes or hours.

EXHIBIT B-1



User Site Hardware Services (USHS) - Those offerings provided by processing services vendors which place programmable hardware at the user's site, rather than at the vendor's data center. Some vendors in the federal government market provide this service under the label of distributed data services. USHS offers the following:

- Access to a communications network
- Access through the network to the RCS vendor's larger computers
- Local management and storage of a data base subset that will serve local terminal users via the connection of a data base processor to the network
- Significant software as part of the service
- *Utility Processing* - Vendor provides access to basic software tools, enabling the users to develop their own problems solutions such as language compilers assemblers, DBMS, sorts scientific library routines, and other systems software.

Other processing services include the following:

- *Batch Services* - These include data processing at vendors' sites for user programs and/or data that are physically transported (as opposed to transported electronically by telecommunications media) to and/or from those sites. Data entry and data output services, such as keypunching and computer output microfilm processing, are also included. Batch services include expenditures by users who take their data to a vendor site with a terminal connected to a remote computer for the actual processing. Other services also includes disaster recovery and backup services.
- *Systems Operations (Processing)* - Also referred to as Resource Management, Facilities Management or COCO (contractor-owned, contractor-operated). Systems control is the management of all or part of a user's data processing functions under a long-term contract of not less than one year. This would include remote computing and batch services. To qualify, the contractor must directly plan, control, operate, and own the facility provided to the user, either onsite, through communications lines, or in a mixed mode.

  Processing services are further differentiated as follows:

  - Cross-industry services involve the processing of applications targeted to specific user departments (e.g., finance, personnel, sales) but cutting across industry lines. Most general-ledger, accounts receivable, payroll, and personnel applications fall into this category.

Cross-industry data base services, for which the vendor supplies the data base and controls access to it (although it may be owned by a third party), are included in this category. General-purpose tools such as financial planning systems, linear regression packages, and other statistical routines are also included. When the application, tool, or data base is designed for specific industry use, however, the services are industry-specific (see below).

- Industry-specific services provide processing for particular functions or problems unique to an industry or industry group. Specialty applications can be used for either business or scientific purposes. Industry-specific data base services, for which the vendor supplies the data base and controls access to it (although it may be owned by a third party), are also included under this category. Examples of industry-specialty applications are seismic data processing, numerically controlled machine tool software development, and demand deposit accounting.

Network services include a wide variety of network-based functions and operations. The common thread is that more of these functions could be performed without network involvement. Network services is divided into two segments: value-added networks (enhanced services) and network applications (electronic information systems).

- *Value-Added Networks (VANs)* - VANs typically involve common carrier network transmission facilities augmented by computerized switches. These networks have become associated with packet-switching technology because the public VANs that have received the most attention (e.g., Telenet and TYMNET) employ packet-switching techniques. But other added data service features such as store-and-forward message switching, terminal interfacing, error detection and correction, and host computer interfacing are of equal importance.

- Network applications include Electronic Data Interchange (EDI), the application-to-application electronic communications between organizations, based on established business document standards, and electronic mail.

Software products - This category comprises user purchases of applications and systems software packages for in-house computer systems. Included are expenditures for lease and purchase, and for work performed by the vendor to implement or maintain the package at the user's sites. Expenditures for work performed by organizations other than the package vendor are counted in the category of professional services. Fees for work related to education, consulting, and/or custom modification of software products are counted as professional services, provided such fees are charged separately from the price of the software product itself. Software products have several subcategories, as indicated below and shown in detail in Exhibit B-2.

EXHIBIT B-2

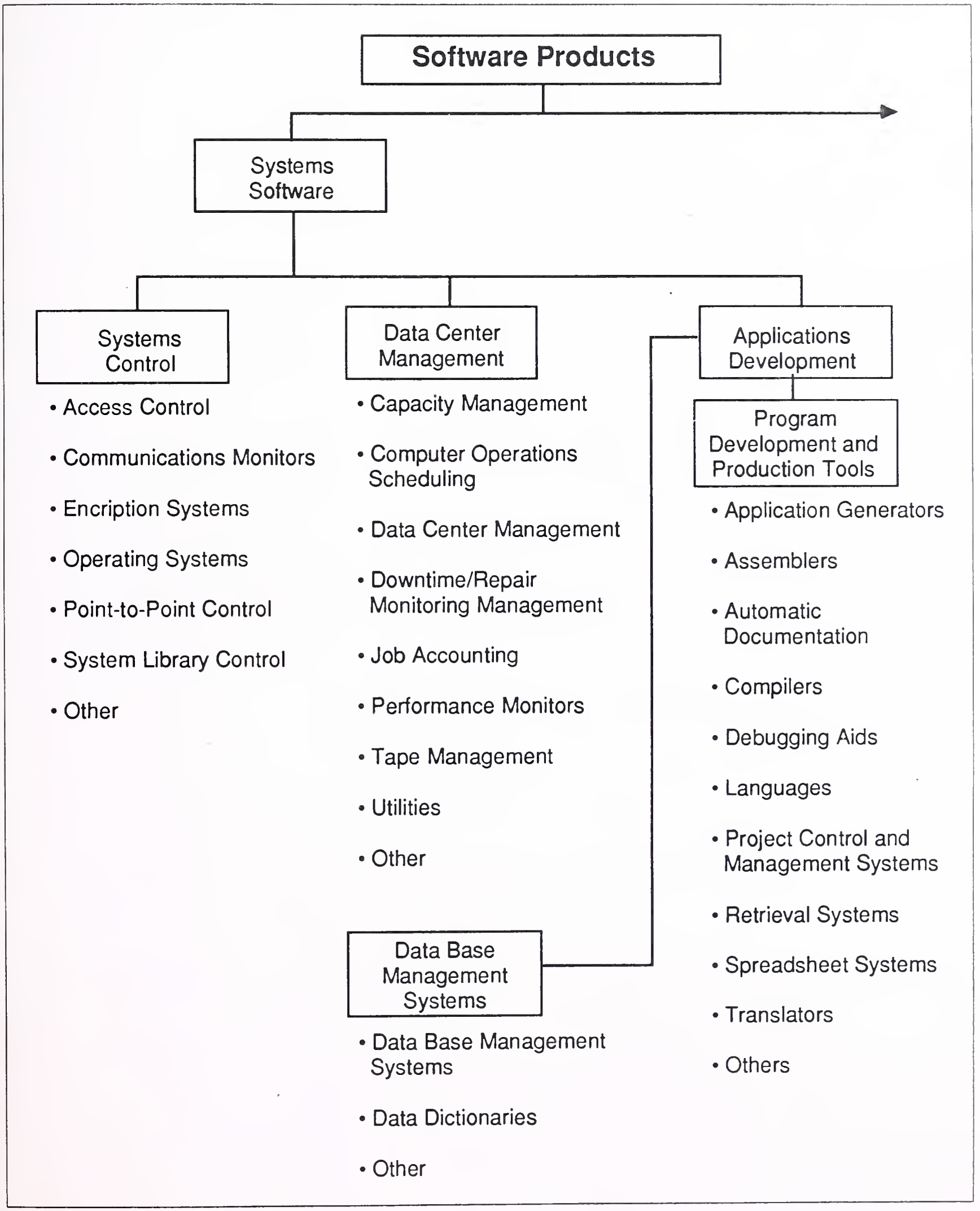
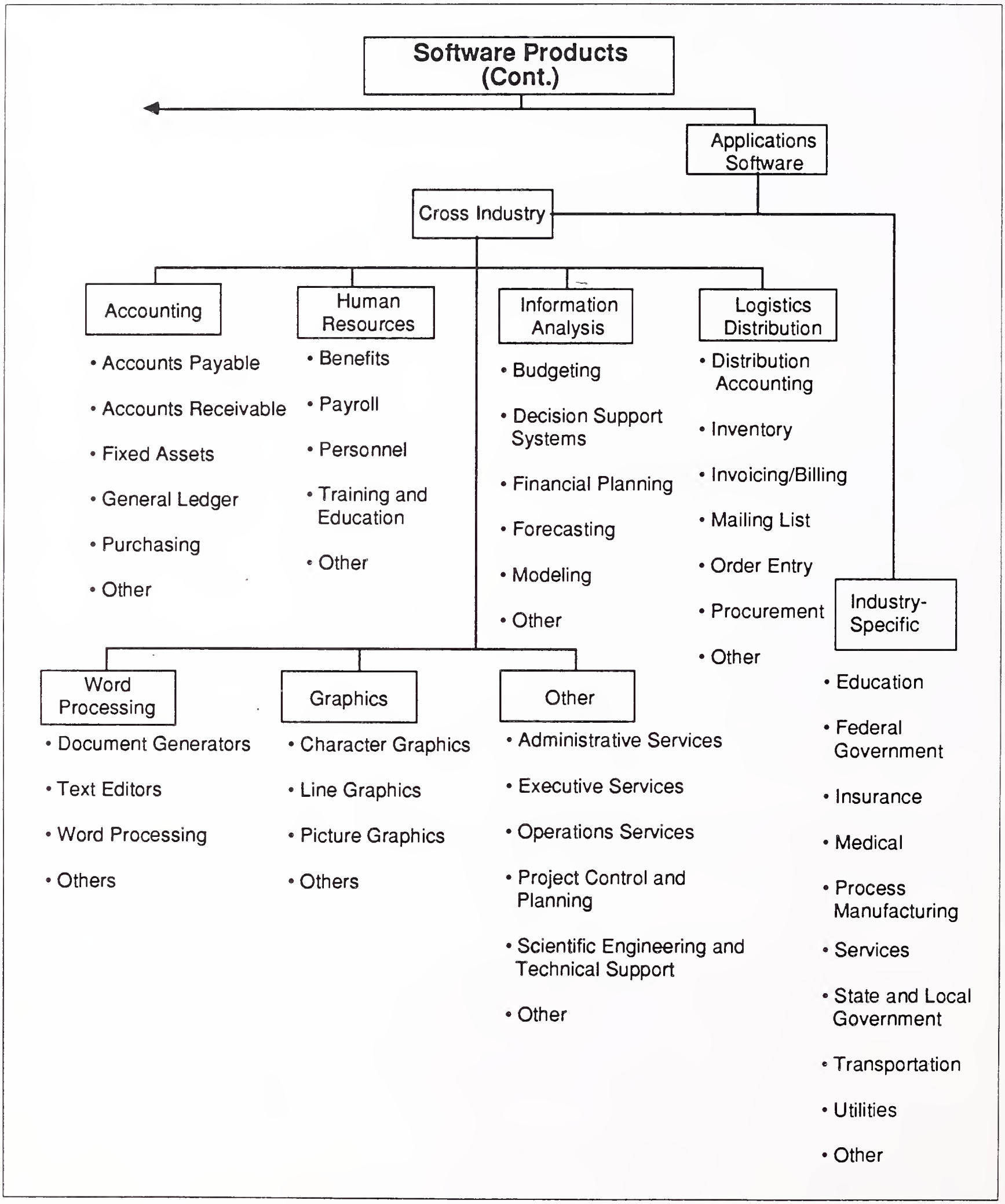


EXHIBIT B-2 (Cont.)



- *Applications Products* - Software that performs functions directly related to solving user's business or organizational need. The products can be any of the following:

  - *Cross-Industry Products* - Used in multiple-industry applications as well as the federal government sector. Examples are payroll, inventory control, and financial planning.

  - *Industry-Specific Products* - Used in a specific industry sector, such as banking and finance, transportation, or discrete manufacturing. Examples are demand deposit accounting, airline scheduling, and material resource planning.

- *Systems Software Products* - Software enabling the computer/communications system to perform basic functions. These products include the following:

  - *System Control Products* - Function during applications program execution to manage the computer system resources. Examples include operating systems, communications monitors, emulators, spoolers, network control, library control, windowing, and access control.

  - *Data Center Management Products* - Used by operations personnel to manage the computer systems resources and personnel more effectively. Examples include performance measurement, job accounting, computer operations scheduling, utilities, and capacity management.

  - *Applications Development Products* - Used to prepare applications for execution by assisting in designing, programming, testing, and related functions. Examples include traditional programming languages, 4GLs, sorts, productivity aids, assemblers, compilers, data dictionaries, data base management systems, report writers, project control, and CASE systems.

Professional Services - This category includes consulting, education and training, software development, and systems operations, as defined below:

- *Software Development* - Develops a software system on a custom basis. It includes one or more of the following: user requirements definition, system design, contract, programming, and/or documentation.

- *Education and Training* - Products and/or services related to information systems and services for the user, including computer-aided instruction (CAI), computer-based education (CBE), and vendor instruction of user personnel in operations, programming, and maintenance

- *Consulting Services* - Information systems and/or services management consulting, project assistance (technical and/or management), feasibility analyses, and cost-effectiveness trade-off studies

- *Systems Operations (Professional Services)* - This is a counterpart to systems operations (professional services) except the computing equipment is owned or leased by the client, not by the vendor. The vendor provides the staff to operate, maintain, and manage the client's facility.

Turnkey Systems - A turnkey system is an integration of systems and applications software with CPU hardware and peripherals, packaged as a single application (or set of applications) solution. The value added by the vendor is primarily in the software and support. Most CAD/CAM systems and many small-business systems are turnkey systems. This does not include specialized hardware systems such as word processors, cash registers, or process control systems; nor does it include Embedded Computer Resources for military applications. They may be either custom or packaged systems.

- Hardware vendors that combine software with their own general-purpose hardware are not classified by INPUT as turnkey vendors. Their software revenues are included in the appropriate software category.

- Turnkey systems revenue is divided into two categories:

  - *Industry-specific systems* - Systems serving a specific function for a given industry sector such as automobile dealer parts inventory, CAD/CAM systems, or discrete manufacturing control systems

  - *Cross-industry systems* - Systems providing a specific function applicable to a wide range of industry sectors, such as financial planning systems, payroll systems, or personnel management systems

- Revenue includes hardware, software, and support functions.

Systems Integration - (SI) delivery of large, complex multidisciplinary, multivendor systems, incorporating some or all of these categories: systems design, programming, integration, equipment, packaged software, communication networks, installation, education and training, and SI related professional services and acceptance. Systems integration contracts typically take more than a year to complete, and involve a prime contractor assuming risk and accepting full responsibility.

B

Hardware/Hardware Systems

Hardware - Includes all computer and telecommunications equipment that can be separately acquired with or without installation by the vendor and not acquired as part of an integrated system

- *Peripherals* - Includes all input, output, communications, and storage devices (other than main memory) that can be connected locally to the main processor, and generally cannot be included in other categories such as terminals

- *Input Devices* - Includes keyboards, numeric pads, card readers, light pens and track balls, tape readers, position and motion sensors, and analog-to-digital converters

- *Output Devices* - Includes printers, CRTs, projection television screens, micrographics processors, digital graphics, and plotters

- *Communication Devices* - Includes modem, encryption equipment, special interfaces, and error control

- *Storage Devices* - Includes magnetic tape (reel, cartridge, and cassette), floppy and hard disks, solid state (integrated circuits), and bubble and optical memories

Terminals - Three types of terminals are described below:

- *User Programmable* - Also called intelligent terminals, including the following:

  - Single-station or standalone
  - Multistation, shared processor
  - Teleprinter
  - Remote batch

- *User Nonprogrammable*

  - Single-station
  - Multistation, shared processor
  - Teleprinter

- *Limited Function* - Originally developed for specific needs, such as point-of-sale (POS), inventory data collection, controlled access, and other applications

Hardware Systems - Includes all processors from microcomputers to supercomputers. Hardware systems may require type- or model-unique

operating software to be functional, but this category excludes applications software and peripheral devices, other than main memory and processors or CPUs not provided as part of an integrated (turnkey) system.

- *Microcomputer* - Combines all of the CPU, memory, and peripheral functions of an 8-, 16-, or 32-bit computer on a chip in various forms including:

  - Integrated circuit package

  - Plug-in boards with increased memory and peripheral circuits

  - Console including keyboard and interfacing connectors

  - Personal computer with at least one external storage device directly addressable by the CPU

  - An embedded computer which may take a number of shapes or configurations

- *Midsize Computer* - Typically a 32- or 64-bit computer with extensive applications software and a number of peripherals in stand-alone or multiple-CPU configurations for business (administrative, personnel, and logistics) applications; also called a general purpose computer. All Intel 80386, Motorola 68000-based systems, and large multiuser systems are included. Specific systems in this category are as follows: IBM 93XX systems; all Digital VAX series systems; and such common UNIX-based systems as those from Apollo and Sun are also included. Most large, shared-logic, integrated office systems—such as those from Wang, Hewlett-Packard, and Honeywell Bull—would also be considered midsized systems. However, this category does not include microcomputers (standalone, or shared), embedded systems, or CAD/CAM systems.

- *Large Computer* - Presently centered on storage controllers, but likely to become bus-oriented and to consist of multiple processors or parallel processor. Intended for structured mathematical and signal processing and typically used with general purpose, Von Neumann-type processors for system control. This term usually refers to traditional mainframes and supercomputers.

- *Supercomputer* - High-powered processors with numerical processing throughput that is significantly greater than the fastest general purpose computers, with capacities in the 100-500 million floating point operations per second (MFLOPS) range. Newer supercomputers, with burst modes over 500 MFLOPS, main storage size up to 10 million words, and on-line storage in the one-to-four gigabyte class, are labeled Class V to Class VII in agency long-range plans. Supercomputers fit in one of two categories:

- *Real Time* - Generally used for signal processing in military applications

- *Non-Real Time* - For scientific use in one of three configurations:

  · Parallel processors
  · Pipeline processor
  · Vector processor

- *Supercomputer* - Term applied to micro, mini, and large mainframe computers with performance substantially higher than attainable by Von Neumann architectures

• *Embedded Computer* - Dedicated computer system designed and implemented as an integral part of a weapon, weapon system, or platform; critical to a military or intelligence mission such as command and control, cryptological activities, or intelligence activities. Characterized by military specifications (MIL SPEC) appearance and operation, limited but reprogrammable applications software, and permanent or semipermanent interfaces. These systems may vary in capacity from microcomputers to parallel processor computer systems.

C

Telecommunications

Networks - Electronic interconnection between sites or locations; may incorporate links between central computer sites and remote locations and switching and/or regional data processing nodes. Network services typically are provided on a leased basis by a vendor to move data, voice, video, or textual information between locations. Networks can be categorized in several different ways:

• *Common Carrier Network* - A public access network, such as AT&T, consisting of conventional, voice-grade circuits and regular switching facilities reached by dial-up calling with leased or user-owned modems for transfer rates between 150 and 1200 baud

• *Value-Added Network (VAN)* - (See listing under Section B, Delivery Modes.)

• *Local-Area Network (LAN)* - Limited-access network between computing resources in a relatively small (but not contiguous) area, such as a building, complex of buildings, or buildings distributed within a metropolitan area. LANs use one of two signaling methods:

  - *Baseband* - Signaling using digital waveforms on a single-frequency band, usually at voice frequencies and bandwidth, and limited to a single sender at any given moment. When used for local-area networks, a baseband is typically used with TDM to permit multiple access.

- *Broadband* - Transmission facilities that use frequencies greater than normal voice-grade, supported in local-area networks with RF modems and AC signaling. Also known as wideband. Employs multiplexing techniques that increase carrier frequency between terminals to provide various services:

  · Multiple (simultaneous) channels via FDM (Frequency Division Multiplexing)

  · Multiple (time-sequenced) channels via TDM (Time Division Multiplexing)

  · High-speed data transfer rate via parallel mode at rates of up to 96,000 baud (or higher, depending on media)

  · *Wide-Area Network (WAN)* - Limited access network between computing resources in buildings, complexes of buildings, or buildings within a large metropolitan or wide geographical area. WANs use baseband or broadband signaling methods.

- *Transmission Facilities* - Includes wire, carrier, coaxial cable, microwave, optical fiber, satellites, cellular radio, and marine cable operating in one of two modes depending on the vendor and the distribution of the network

  - *Mode* - may be either analog or digital:

    · *Analog* - Transmission or signal with continuous-waveform representation, typified by AT&T's predominantly voice-grade DDD network and most telephone operating company distribution systems

    · *Digital* - Transmission or signal using discontinuous, discrete quantities to represent data, record, video, or text in binary form

  • *Media* - may be any of the following:

    - *Wire* - Varies from earlier, single-line, teletype networks, to two-wire standard telephone (twisted pair), to four-wire, full-duplex, balanced lines

    - *Carrier* - A wave, pulse train, or other signal suitable for modulation by an information-bearing signal to be transmitted over a communications system, used in multiplexing applications to increase network capacity

    - *Coaxial Cable* - A cable used in HF (high-frequency) and VHF (very high frequency), single-frequency, or carrier-based systems, which

requires frequent reamplification (repeaters) to carry the signal any distance

- *Microwave* - UHF (ultra-high-frequency) multichannel, point-to-point, repeated radio transmission, also capable of wide frequency channels

- *Optical Fiber* - Local signal distribution systems employed in limited areas, using light-transmitting glass fibers and TDM for multichannel applications

- *Communications Satellites* - Synchronous, earth-orbiting systems that provide point-to-point, two-way service over significant distances without intermediate amplification (repeaters), but requiring suitable groundstation facilities expand markets for those technologies, and leverage existing and new product lines. In effect, they are focused on using their typically limited professional services resources to maximize the return on their core business products. This is true in most cases for federal market vendors as well. Most hardware firms prefer to apply their own core business products, and cannot avoid the use of the hardware of other manufacturers. This policy may limit their ability to respond to all systems integration asynchronous or synchronous, half or full duplex.

D

General Definitions

ASCII - American National Standard Code for Information Interchange—Eight-bit code with seven data bits and one parity bit

Asynchronous - Communications operation (such as transmission) without continuous timing signals. Synchronization is accomplished by appending signal elements to the data.

Bandwidth - Range of transmission frequencies that can be carried on a communications path; used as a measure of capacity.

Baud - Number of signal events (discrete conditions) per second. Typically used to measure modem or terminal transmission speed.

Byte - Usually equivalent to the storage required for one alphanumeric character (i.e., one letter or number)

CBX - Computerized Branch Exchange—A PABX based on a computer system, implying programmability and usually voice and data capabilities

Central Processing Unit (CPU) - The arithmetic and control portion of a computer; i.e., the circuits controlling the interpretation and execution of computer instructions.

Centrex - Central office telephone services that permit local circuit switching without installation of customer premises equipment. Could be described as shared PBX service.

Circuit Switching - A process that, usually on demand, connects two or more network stations, and permits exclusive circuit use until the connection is released; typical of the voice telephone network, where a circuit is established between the caller and the called party.

CO - Central Office—Local telco site for one or more exchanges

CODEC - Coder/decoder, equivalent to modem for digital devices

Constant Dollars - Growth forecasts in constant dollars make no allowance for inflation or recession. Dollar value based on the year of the forecast unless otherwise indicated.

Computer System - The combination of computing resources required to perform the designed functions. May include one or more CPUs, machine room peripherals, storage systems, and/or applications software.

CPE - Customer Premises Equipment—DCE or DTE located at a customer site rather than at a carrier site such as the local telephone company CO. May include switchboards, PBX, data terminals, and telephone answering devices.

CSMA/CD - Carrier Sense Multiple Access/Collision Detect—Contention protocol used in local-area networks, typically with a multipoint configuration

Current Dollars - Estimates or values expressed in current-year dollars which, for forecasts, would include an allowance for inflation

Data Encryption Standard (DES) - Fifty-six-bit key, one-way encryption algorithm adopted by NIST in 1977, implemented through hardware ("S-boxes") or software. Designed by IBM with NSA guidance.

Datagram - A self-contained packet of information that does not depend on the contents of preceding or following packets and has a finite length

DCA - IBM's Document Content Architecture—Protocols for specifying document (text) format which are consistent across a variety of hardware and software systems within IBM's DISOSS

DCE - Data Circuit-terminating Equipment—Interface hardware that couples DTE to a transmission circuit or channel by providing functions to establish, maintain, and terminate a connection, including signal conversion and coding

DDCMP - Digital Data Communications Message Protocol —Data link protocol used in Digital Equipment Company's DECNET

DECNET - Digital Equipment Company's network architecture

Dedicated Circuit - A permanently established network connection between two or more stations; contrast with switched circuit

DEMS - Digital Electronic Message Service—Nationwide common carrier digital networks which provide high-speed, end-to-end, two-way transmission of digitally encoded information using the 10.6 GHz band

DIA - IBM's Document Interchange Architecture - Protocols for transfer of documents (text) between different hardware and software systems within IBM's DISOSS

DISOSS - IBM's DIStributed Office Support System - Office automation environment, based on DCA and DIA, which permits document (text) transfer between different hardware and software systems without requiring subsequent format or content revision

Distributed Data Processing - The development of programmable intelligence in order to perform a data processing function where it can be accomplished most effectively through computers and terminals arranged in a telecommunications network adapted to the user's needs

DTE - Data Terminal Equipment—Hardware which is a data source, link, or both, such as video display terminals that convert user information into data transmission, and reconvert data signals into user information

EBCDIC - Extended Binary Coded Decimal Interchange Code —Eight-bit code typically used in IBM mainframe environments

EFT - Electronic funds transfer

Encryption - Electric, code-based conversion of transmitted data to provide security and/or privacy of data between authorized access points

End User - One who is using a product or service to accomplish his or her own functions. The end user may buy a system from the hardware supplier(s) and do his or her own programming, interfacing, and installation. Alternately, the end user may buy a turnkey system from a systems house or hardware integrator, or may buy a service from an in-house department or external vendor.

Engineering Change Notice (ECN) - Product improvements after production

Engineering Change Order (ECO) - The follow-up to ECNs, including parts and a bill of materials to effect the change in the hardware

Equipment Operators - Individuals operating computer control consoles and/or peripheral equipment (BLS definition)

Ethernet - Local-area network developed by Xerox PARC using base-band signaling, CSMA/CD protocol, and coaxial cable to achieve a 10 mbps data rate

Facsimile - Transmission and reception of graphic data, usually fixed images of documents, through scanning and conversion of a picture signal

FDM - Frequency Division Multiplexing—A multiplexing method that permits multiple access by assigning different frequencies of the available bandwidth to different channels

FEP - Front-End Processor—Communications concentrator such as the IBM 3725 or COMTEN 3690 used to interface communications lines to host computers

Field Engineer (FE) - Field engineer, customer engineer, serviceperson, and maintenance person are used interchangeably and refer to the individual who responds to a user's service call to repair a device or system.

Full-Duplex - Bi-directional communications, with simultaneous, two-way transmission

General Purpose Computer System - A computer designed to handle a wide variety of problems. Includes machine room peripherals, systems software, and small business systems.

Half-Duplex - Bi-directional communications, but only in one direction at a time

Hardware Integrator - Develops system interface electronics and controllers for the CPU, sensors, peripherals, and all other ancillary hardware components. The hardware integrator also may develop control system software in addition to installing the entire system at the end-user site.

HDLC - High-level Data Link Control

Hertz- Number of signal oscillations (cycles) per second, abbreviated Hz

IBM Token Ring - IBM's local area network using baseband signalling and operating at 4 mbps on twisted-pair copper wire. Actually a combination of star and ring topologies—IEEE 802.5-compatible.

IDN - Integrated Digital Network—Digital switching and transmission; part of the evolution to ISDN.

Independent Suppliers - Suppliers of machine room peripherals, though usually not suppliers of general purpose computer systems

Information Processing - Data processing as a whole, including use of business and scientific computers

Installed Base - Cumulative number or value (cost when new) of computers in use

Interconnection - Physical linkage between devices on a network

Interoperability - The capability to operate with other devices on a network. Different from interconnection, which merely guarantees a physical network interface.

ISDN - Integrated Services Digital Network—Completely digital, integrated voice and nonvoice public network service. Not clearly defined through any existing standards, although FCC and other federal agencies are developing CCITT recommendations.

Keypunch Operators - Individuals operating keypunch machines (similar to electric typewriters) to transcribe data from source materials onto punch cards

Lease Line - Permanent connection between two network stations. Also known as dedicated or non-switched line.

Machine Repairers - Individuals who install and periodically service computer systems

Machine Room Peripherals - Peripheral equipment generally located close to the central processing unit

Mainframe - The central processing unit (CPU or units in a parallel processor) of a computer that interprets and executes computer (software) instructions of 32 bits or more

MAP - Manufacturing Automation Protocol - Seven-layer communications standard for factory environments promoted by General Motors/ EDS. Adopts IEEE 802.2 and IEEE 802.4 standards plus OSI protocols for other layers of the architecture.

Mean Time to Repair - The mean of elapsed times from the arrival of the field engineer on the user's site to the time when the device is repaired and returned to user service

Mean Time to Respond - The mean of elapsed times from the user call for services and the arrival of the field engineer on the user's site

Message - A communication intended to be read by a person. The quality of the received document need not be high, only readable. Graphic materials are not included.

MMFS - Manufacturing Messaging Format Standard—Application-level protocol included within MAP

Modem - A device that encodes information into electronically transmittable form (MOdulator) and restores it to original analog form (DEModulator)

NCP - Network Control Program—Software used in IBM 3705/3725 FEPs for control of SNA networks.

Node - Connection point of three or more independent transmission points which may provide switching or data collection

Off-Line - Pertaining to equipment or devices that can function without direct control of the central processing unit

On-Line - Pertaining to equipment or devices under direct control of the central processing unit

OSI - ISO reference model for Open Systems Interconnection—Seven-layer architecture for application, presentation, session, transport, network, data link, and physical services and equipment

OSI Application Layer - Layer 7, providing end-user applications services for data processing

OSI Data Link Layer - Layer 2, providing transmission protocols, including frame management, link flow control, and link initiation/release

OSI Network Layer - Layer 3, providing call establishment and clearing control through the network nodes

OSI Physical Layer - Layer 1, providing the mechanical, electrical, functional, and procedural characteristics to establish, maintain, and release physical connections to the network

OSI Presentation Layer - Layer 6, providing data formats and information such as data translation, data encoding/decoding, and command translation

OSI Session Layer - Layer 5, establishes, maintains, and terminates logical connections for the transfer of data between processes

OSI Transport Layer - Layer 4, providing end-to-end terminal control signals such as acknowledgements

Overseas - Not within the geographical limits of the continental United States, Alaska, Hawaii, and U.S. possessions

PABX - Private Automated Branch Exchange—Hardware that provides automatic (electro-mechanical or electronic) local circuit switching on a customer's premises

PAD - Packet Assembler-Disassembler—A device that enables DTE not equipped for packet switching operation to operate on a packet switched network

PBX - Private Branch Exchange—Hardware that provides local circuit switching on the customer premise

PCM - Pulse-Code Modulation—Modulation involving conversion of a waveform from analog to digital form through coding

PDN - Public Data Network—A network established and operated by a recognized private operating agency, a telecommunications administration, or other agency for the specific purpose of providing data transmission services to the public

Peripherals - Any unit of input/output equipment in a computer system, exclusive of the central processing unit

PPM - Pulse Position Modulation

Private Network - A network established and operated for one user or user organization

Programmers - Persons mainly involved in designing, writing, and testing computer software programs

Protocols - The rules for communication system operation that must be followed if communication is to be effected. Protocols may govern portions of a network or service. In digital networks, protocols are digitally encoded as instructions to computerized equipment.

Public Network - A network established and operated for more than one user with shared access, usually available on a subscription basis. See related international definition of PDN.

Scientific Computer System - A computer system designed to process structured mathematics (such as Fast Fourier Transforms), and complex, highly redundant information (such as seismic data, sonar data, and radar), with large, on-line memories and very high-capacity output

SDLC - Synchronous Data Link Control—IBM's data link control for SNA. Supports a subset of HDLC modes.

SDN - Software-Defined Network

Security - Physical, electrical, and computer (digital) coding procedures to protect the contents of computer files and data transmission from inadvertent or unauthorized disclosure to meet the requirements of the Privacy Act and national classified information regulations

Service Delivery Point - The location of the physical interface between a network and customer/user equipment

Simplex - Unidirectional communications

Smart Box - A device for adapting existing DTE to new network standards such as OSI. Includes PADs and protocol convertors, for example.

SNA - Systems Network Architecture—Seven-layer communications architecture designed by IBM. Layers correspond roughly but not exactly to OSI model.

Software - Computer programs

Supplies - Includes materials associated with the use of operations of computer systems, such as printer paper, keypunch card, disk packs, and tapes

Switched Circuit - Temporary connection between two network stations established through dial-up procedures

Synchronous - Communications operation with separate, continuous clocking at both sending and receiving stations

Systems Analyst - Individual who analyzes problems to be converted to a programmable form for application to computer systems

Systems House - Vendor that acquires, assembles, and integrates hardware and software into a total system to satisfy the data processing requirements of an end user. The vendor also may develop systems software products for license to end users. The systems house vendor does not manufacture mainframes.

Systems Integrator - Systems house vendor that develops systems interface electronics, applications software, and controllers for the CPU, peripherals, and ancillary subsystems which may have been provided by a contractor or the government (GFE). This vendor may either supervise or perform the installation and testing of the completed system.

T1 - Bell System designation for 1.544 mbps carrier capable of handling 24 PCM voice channels

TDM - Time Division Multiplexing—A multiplexing method that interleaves multiple transmissions on a single circuit by assigning a different time slot to each channel.

Token Passing - Local-area network protocol which allows a station to transmit only when it has the "token," an empty slot on the carrier

TOP - Technical Office Protocol —Protocol developed by Boeing Computer Services to support administrative and office operations as complementary functions to factory automation implemented under MAP

Turnkey System - System composed of hardware and software integrated into a total system designed to fulfill completely the processing requirements of a single application

Twisted-Pair Cable - Communications cabling consisting of pairs of single-strand metallic electrical conductors, such as copper wires, typically used in building telephone wiring and some LANs

Verification and Validation - Process for examining and testing applications and special systems software to verify that it operates on the target CPU and performs all of the functions specified by the user

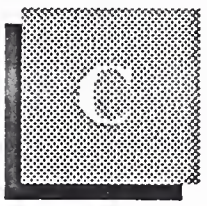
Voice-Grade - Circuit or signal in the 300-3300 Hz bandwidth typical of the public telephone system, nominally a 4 Khz user

VTAM - Virtual Telecommunications Access Method—Host-resident communications software for SNA networks

E

Other Considerations

When questions arise as to the proper place to count certain user expenditures, INPUT addresses the questions from the user viewpoint. Expenditures are then categorized according to the users' perception of the purchase.



Glossary of Acronyms

The federal government's procurement language uses a combination of acronyms, phrases, and words that is complicated by different agency definitions and interpretations. The government also uses terms of accounting, business, economics, engineering, and law with new applications and technology.

Acronyms and contract terms that INPUT encountered most often in program documentation and interviews for this report are listed below, but this glossary should not be considered all-inclusive. Federal procurement regulations (DAR, FPR, FAR, FIRMR, FPMR) and contract terms listed in RFIs, RFPs, and RFQs provide applicable terms and definitions.

Federal agency acronyms have been included if they are used in this report.

A

Federal Acronyms

AAS	Automatic Addressing System.
AATMS	Advanced Air Traffic Management System.
ACO	Administrative Contracting Offices (DCAS).
ACS	Advanced Communications Satellite (formerly NASA 30/20 GHz Satellite Program).
ACT-1	Advanced Computer Techniques (Air Force).
Ada	DoD High-Order Language.
ADA	Airborne Data Acquisition.
ADL	Authorized Data List.
ADS	Automatic Digital Switches (DCS).
AFA	Air Force Association.
AFCEA	Armed Forces Communications Electronics Association.
AGE	Aerospace Ground Equipment.
AIP	Array Information Processing.
AIS	Automated Information System.
AMPE	Automated Message Processing Equipment.

AMPS	Automated Message Processing System.
AMSL	Acquisition Management Systems List.
ANG	Army National Guard.
AP(P)	Advance Procurement Plan.
Appropriation	Congressionally approved funding for authorized programs and activities of the Executive Branch.
APR	Agency Procurement Request.
ARPANET	DARPA network of scientific computers.
ASP	Aggregated Switch Procurement.
ATLAS	Abbreviated Test Language for All Systems (for ATE-Automated Test Equipment).
Authorization	In the legislative process programs, staffing and other routine activities must be approved by Oversight Committees before the Appropriations Committee will approve the money from the budget.
AUSA	Association of the U.S. Army.
AUTODIN	AUTOmatic DIgital Network of the Defense Communications System.
AUTOSEVOCOM	AUTOmatic SEcure VOice Communications Network
AUTOVON	AUTOmatic VOice Network of the Defense Communications System.
BA	Basic Agreement.
BAFO	Best And Final Offer.
Baselevel	Procurement, purchasing, and contracting at the military installation level.
BCA	Board of Contract Appeals.
Benchmark	Method of evaluating ability of a candidate computer system to meet user requirements.
Bid protest	Objection (in writing, before or after contract award) to some aspect of a solicitation by a valid bidder.
BML	Bidders Mailing List—Qualified vendor information filed annually with federal agencies to receive automatically RFPs and RFQs in areas of claimed competence.
BOA	Basic Ordering Agreement.
B&P	Bid and Proposal—Vendor activities in response to solicitation/specific overhead allowance.
BPA	Blanked Purchase Agreement.
Budget	Federal Budget, proposed by the President and subject to Congressional review.
C^2	Command and Control.
C^3	Command, Control, and Communications.
C^4	Command, Control, Communications, and Computers.
C^3I	Command, Control, Communications, and Intelligence.
CAB	Contract Adjustment Board or Contract Appeals Board.
CADE	Computer-Aided Design and Engineering.

CADS	Computer-Assisted Display Systems.
CAIS	Computer-Assisted Instruction System.
CALS	Computer-Aided Automated Logistics System.
CAPS	Command Automation Procurement Systems.
CAS	Contract Administration Services or Cost Accounting Standards.
CASB	Cost Accounting Standards Board.
CASP	Computer-Assisted Search Planning.
CBD	*Commerce Business Daily*—U.S. Department of Commerce publication listing government contract opportunities and awards.
CBO	Congressional Budget Office.
CCEP	Commercial Comsec Endorsement Program.
CCDR	Contractor Cost Data Reporting.
CCN	Contract Change Notice.
CCPDS	Command Center Processing and Display Systems.
CCPO	Central Civilian Personnel Office.
CCTC	Command and Control Technical Center (JCS).
CDR	Critical Design Review.
CDRL	Contractor Data Requirement List.
CFE	Contractor-Furnished Equipment.
CFR	Code of Federal Regulations.
CICA	Competition in Contracting Act.
CIG	Computerized Interactive Graphics.
CIR	Cost Information Reports.
CM	Configuration Management.
CMI	Computer-Managed Instruction.
CNI	Communications, Navigation, and Identification.
CO	Contracting Office, Contract Offices, or Change Order.
COC	Certificate of Competency (administered by the Small Business Administration).
COCO	Contractor-Owned, Contractor-Operated.
CODSIA	COuncil of Defense and Space Industry Associations.
COMSTAT	Communications Satellite Corporation.
CONUS	CONtinental U. S.
COP	Capability Objective Package.
COTR	Contracting Officer's Technical Representative.
CP	Communications Processor.
CPAF	Cost-Plus-Award-Fee contract.
CPFF	Cost-Plus-Fixed-Fee contract.
CPIF	Cost-Plus-Incentive-Fee contract.
CPR	Cost Performance Reviews.
CPSR	Contractor Procurement System Review.
CR	Cost Reimbursement (Cost Plus contract).
CSA	Combat or Computer Systems Architecture.
C/SCSC	Cost/Schedule Control System Criteria (also called "C-Spec").
CWAS	Contractor Weighted Average Share in Cost Risk.

DAL	Data Accession List.
DAR	Defense Acquisition Regulations.
DARPA	Defense Advanced Research Projects Agency.
DAS	Data Acquisition System.
DBHS	Data Base Handling System.
DCA	Defense Communications Agency.
DCAA	Defense Contract Audit Agency.
DCAS	Defense Contract Administration Services.
DCASR	DCAS Region.
DCC	Digital Control Computer.
DCP	Development Concept Paper (DoD).
DCS	Defense Communications System.
DCTN	Defense Commercial Telecommunications Network.
DDA	Dynamic Demand Assessment (Delta Modulation).
DDC	Defense Documentation Center.
DDL	Digital Data Link—A segment of a communications network used for digital data transmission.
DDN	Defense Data Network.
DDS	Dynamic Diagnostics System.
DECCO	DEfense Commercial Communications Office.
DECEO	DEfense Communications Engineering Office.
D&F	Determination and Findings—Required documentation for approval of a negotiated procurement.
DIA	Defense Intelligence Agency.
DIF	Document Interchange Format—Navy-sponsored word processing standard.
DHHS	Department of Health and Human Services.
DIDS	Defense Integrated Data Systems
DISC	Defense Industrial Supply Center.
DLA	Defense Logistics Agency.
DMA	Defense Mapping Agency.
DNA	Defense Nuclear Agency.
DO	Delivery Order.
DOA	Department of Agriculture (also USDA).
DOC	Department of Commerce.
DOE	Department of Energy.
DOI	Department of Interior.
DOJ	Department of Justice.
DOS	Department of State.
DOT	Department of Transportation.
DPA	Delegation of Procurement Authority (granted by GSA under FPRs).
DPC	Defense Procurement Circular.
DQ	Definite Quantity Contract.
DQ/PL	Definite Quantity Price List Contract.
DR	Deficiency Report.
DSCS	Defense Satellite Communication System.
DSN	Defense Switched Network.
DSP	Defense Support Program (WWMCCS).
DSS	Defense Supply Service.

DTC	Design-To-Cost.
ECP	Engineering Change Proposal.
ED	Department of Education.
EEP	Equal Employment Opportunity.
EMC	Electro-Magnetic Compatibility.
EMCS	Energy Monitoring and Control System.
EO	Executive Order - Order issued by the President.
EOQ	Economic Ordering Quantity.
EPA	Economic Price Adjustment.
EPA	Environmental Protection Agency.
EPMR	Estimated Peak Monthly Requirement.
EPS	Emergency Procurement Service (GSA) or Emergency Power System.
EUC	End User Computing, especially in DoD.
FA	Formal Advertising.
FAC	FAcility Contract.
FAR	Federal Acquisition Regulations.
FCA	Functional Configuration Audit.
FCC	Federal Communications Commission.
FCDC	Federal Contract Data Center.
FCRC	Federal Contract Research Center.
FDPC	Federal Data Processing Center.
FEDSIM	Federal (Computer) SIMulation Center (GSA).
FEMA	Federal Emergency Management Agency.
FFP	Firm Fixed-Price contract (also Lump Sum Contract).
FIPS	NIST Federal Information Processing Standard.
FIPS PUBS	FIPS PUBlications.
FIRMR	Federal Information Resource Management Regulations.
FMS	Foreign Military Sales.
FOC	Final Operating Capability.
FOIA	Freedom of Information Act.
FP	Fixed-Price contract.
FP-L/H	Fixed-Price—Labor/Hour contract.
FP-LOE	Fixed-Price—Level-Of-Effort contract.
FPMR	Federal Property Management Regulations.
FPR	Federal Procurement Regulations.
FSC	Federal Supply Classification.
FSG	Federal Supply Group.
FSN	Federal Supply Number.
FSS	Federal Supply Schedule or Federal Supply Service (GSA).
FSTS	Federal Secure Telecommunications System.
FT Fund	A revolving fund, designated as the Federal Telecommunications Fund, used by GSA to pay for GSA-provided common-user services, specifically including the current FTS and proposed FTS 2000 services.

FTPS	Federal Telecommunications Standards Program administered by NCS; standards are published by GSA.
FTS	Federal Telecommunications System.
FY	Fiscal Year.
FYDP	Five Year Defense Plan.
GAO	General Accounting Office.
GFE	Government-Furnished Equipment.
GFM	Government-Furnished Material.
GFY	Government Fiscal Year.
GIDEP	Government-Industry Data Exchange Program
GOCO	Government-Owned, Contractor-Operated.
GOGO	Government-Owned, Government-Operated.
GOSIP	Government Open Systems Interconnection Profile.
GPO	Government Printing Office.
GPS	Global Positioning System.
GRH	Gramm-Rudman-Hollings Act (1985), also called Gramm-Rudman Deficit Control.
GS	General Schedule.
GSA	General Services Administration.
GSBCA	General Services Administration Board of Contract Appeal.
HCFA	Health Care Financing Administration.
HHS	(Department of) Health and Human Services.
HPA	Head of Procuring Activity.
HSDP	High-Speed Data Processors.
HUD	(Department of) Housing and Urban Development.
ICA	Independent Cost Analysis.
ICAM	Integrated, Computer-Aided Manufacturing.
ICE	Independent Cost Estimate.
ICP	Inventory Control Point.
ICST	Institute for Computer Sciences and Technology, National Institute of Standards and Technology.
IDAMS	Image Display And Manipulation System.
IDEP	Interservice Data Exchange Program.
IDN	Integrated Data Network.
IFB	Invitation For Bids.
IOC	Initial Operating Capability.
IOI	Internal Operating Instructions.
IPS	Integrated Procurement System.
IQ	Indefinite Quantity Contract.
IR&D	Independent Research & Development.
IRM	Information Resource Manager.
IXS	Information Exchange System.
JOCIT	JOvial Compiler Implementation Tool.
JSIPS	Joint Systems Integration Planning Staff.
JSOP	Joint Strategic Objectives Plan.

JSOR	Joint Service Operational Requirement.
JUMPS	Joint Uniform Military Pay System.
LC	Letter Contract.
LCC	Life Cycle Costing.
LCMP	Life Cycle Management Procedures (DD7920.1).
LCMS	Life Cycle Management System.
L-H	Labor-Hour Contract.
LOI	Letter of Interest.
LRPE	Long-Range Procurement Estimate.
LRIRP	Long-Range Information Resource Plan.
MAISRC	Major Automated Information Systems Review Council (DoD).
MANTECH	MANufacturing TECHnology.
MAPS	Multiple Address Processing System.
MAP/TOP	Manufacturing Automation Protocol/Technical and Office Protocol.
MASC	Multiple Award Schedule Contract.
MDA	Multiplexed Data Accumulator.
MENS	Mission Element Need Statement or Mission Essential Need Statement (see DD-5000.1 Major Systems Acquisition).
MILSCAP	MILitary Standard Contract Administration Procedures.
MIL SPEC	MILitary SPECification.
MIL STD	Military Standard.
MIPR	Military Interdepartmental Purchase Request.
MOD	Modification.
MOL	Maximum Ordering Limit (Federal Supply Service).
MPC	Military Procurement Code.
MYP	MultiYear Procurement.
NARDIC	Navy Research and Development Information Center.
NASA	National Aeronautics and Space Administration.
NCMA	National Contract Management Association.
NCS	National Communications System; responsible for setting U.S. Government standards administered by GSA; also holds primary responsibility for emergency communications planning.
NICRAD	Navy-Industry Cooperative Research and Development.
NIP	Notice of Intent to Purchase.
NIST	National Institute of Standards and Technology.
NMCS	National Military Command System.
NSA	National Security Agency.
NSEP	National Security and Emergency Preparedness.
NSF	National Science Foundation.
NSIA	National Security Industrial Association.

NTIA	National Telecommunications and Information Administration of the Department of Commerce; replaced the Office of Telecommunications Policy in 1970 as planner and coordinator for government communications programs; primarily responsible for radio.
NTIS	National Technical Information Service.
Obligation	Earmarking of specific funding for a contract from committed agency funds.
OCS	Office of Contract Settlement.
OFCC	Office of Federal Contract Compliance.
Off-site	Services to be provided near but not in government facilities.
OFMP	Office of Federal Management Policy (GSA).
OFPP	Office of Federal Procurement Policy.
OIRM	Office of Information Resources Management.
O&M	Operations & Maintenance.
OMB	Office of Management and Budget.
OM&R	Operations, Maintenance, and Readiness.
On-site	Services to be performed on a government installation or in a specified building.
OPM	Office of Procurement Management (GSA) or Office of Personnel Management.
Options	Sole-source additions to the base contract for services or goods to be exercised at the government's discretion.
OSHA	Occupational Safety and Health Act.
OSI	Open System Interconnect.
OSP	OffShore Procurement.
OTA	Office of Technology Assessment (Congress).
Out-Year	Proposed funding for fiscal years beyond the budget year (next fiscal year).
P-1	FY Defense Production Budget.
P3I	Pre-Planned Product Improvement (program in DoD).
PAR	Procurement Authorization Request or Procurement Action Report.
PAS	Pre-Award Survey.
PASS	Procurement Automated Source System.
PCO	Procurement Contracting Officer.
PDA	Principal Development Agency.
PDM	Program Decision Memorandum.
PDR	Preliminary Design Review.
PIR	Procurement Information Reporting.
PME	Performance Monitoring Equipment.
PMP	Purchase Mangement Plan.
PO	Purchase Order or Program Office.
POM	Program Objective Memorandum.
POSIX	Portable Open System Interconnect Exchange.

POTS	Purchase of Telephone Systems.
PPBS	Planning, Programming, Budgeting System.
PR	Purchase Request or Procurement Requisition.
PRA	Paperwork Reduction Act.
PS	Performance Specification - alternative to a Statement of Work, when work to be performed can be clearly specified.
QA	Quality Assurance.
QAO	Quality Assurance Office.
QMCS	Quality Monitoring and Control System (DoD software).
QMR	Qualitative Material Requirement (Army).
QPL	Qualified Products List.
QRC	Quick Reaction Capability.
QRI	Quick Reaction Inquiry.
R-1	FY Defense RDT&E Budget.
RAM	Reliability, Availability, and Maintainability.
RC	Requirements Contract.
R&D	Research and Development.
RDA	Research, Development, and Acquisition.
RDD	Required Delivery Date.
RD&E	Research, Development, and Engineering.
RDF	Rapid Deployment Force.
RDT&E	Research, Development, Test, and Engineering.
RFI	Request for Information.
RFP	Request for Proposal.
RFQ	Request for Quotation.
RFTP	Request for Technical Proposals (Two-Step).
ROC	Required Operational Capability.
ROI	Return on Investment.
RTAS	Real Time Analysis System.
RTDS	Real Time Display System.
SA	Supplemental Agreement.
SBA	Small Business Administration.
SB Set-Aside	Small Business Set-Aside contact opportunities with bidders limited to certified small businesses.
SCA	Service Contract Act (1964 as amended).
SCN	Specification Change Notice.
SDN	Secure Data Network.
SEC	Securities and Exchange Commission.
SE&I	Systems Engineering and Integration.
SETA	Systems Engineering/Technical Assistance.
SETS	Systems Engineering/Technical Support.
SIBAC	Simplified Intragovernmental Billing and Collection System.
SIMP	Systems Integration Master Plan.
SIOP	Single Integrated Operations Plan.
SNAP	Shipboard Nontactical ADP Program.

Sole Source	Contract award without competition.
Solicitation	Invitation to submit a bid.
SOR	Specific Operational Requirement.
SOW	Statement Of Work.
SSA	Source Selection Authority (DoD).
SSAC	Source Selection Advisory Council.
SSEB	Source Selection Evaluation Board.
SSO	Source Selection Official (NASA).
STINFO	Scientific and Technical INFOrmation Program—Air Force/NASA.
STU	Secure Telephone Unit.
SWO	Stop-Work Order.
Synopsis	Brief Description of contract opportunity in CBD after D & F and before release of solicitation.
TA/AS	Technical Assistance/Analysis Services.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TEMPEST	Studies, inspections, and tests of unintentional electromagnetic radiation from computer, communication, command, and control equipment that may cause unauthorized disclosure of information; usually applied to DoD and security agency testing programs.
TILO	Technical and Industrial Liasion Office—Qualified Requirement Information Program—Army.
TM	Time and Materials contract.
TOA	Total Obligational Authority (Defense).
TOD	Technical Objective Document.
TR	Temporary Regulation (added to FPR, FAR).
TRACE	Total Risk Assessing Cost Estimate.
TRCO	Technical Representative of the Contracting Offices.
TREAS	Department of the Treasury.
TRP	Technical Resources Plan.
TSP	GSA's Teleprocessing Services Program.
TVA	Tennessee Valley Authority.
UCAS	Uniform Cost Accounting System.
USA	U.S. Army.
USAF	U.S. Air Force.
USCG	U.S. Coast Guard.
USMC	U.S. Marine Corps.
USN	U.S. Navy.
U.S.C.	United States Code.
USPS	United States Postal Service.
USRRB	United States Railroad Retirement Board.
VA	Department of Veterans Affairs.
VE	Value Engineering.
VHSIC	Very High Speed Integrated Circuits.
VIABLE	Vertical Installation Automation Base Line (Army).
VICI	Voice Input Code Identifier.

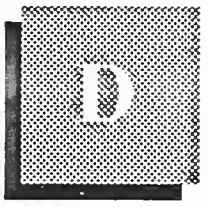
WBS	Work Breakdown Structure.
WGM	Weighted Guidelines Method.
WIN	WWMCCS Intercomputer Network.
WIS	WWMCCS Information Systems.
WITS	Washington Interagency Telecommunications System.
WS	Work Statement—Offerer's description of the work to be done (proposal or contract).
WWMCCS	World-Wide Military Command and Control System.
8(a)	Set-Aside Agency awards direct to Small Business Administration for direct placement with a socially/economically disadvantaged company.

B

General and Industry Acronyms

ADAPSO	Association of Data Processing Service Organization, now the Computer Software and Services Industry Association.
ADP	Automatic Data Processing.
ADPE	Automatic Data Processing Equipment.
ANSI	American National Standards Institute.
BOC	Bell Operating Company.
CAD	Computer-Aided Design.
CAM	Computer-Aided Manufacturing.
CBEMA	Computer and Business Equipment Manufacturers Association.
CCIA	Computers and Communications Industry Association.
CCITT	Comite Consultaif Internationale de Telegraphie et Telephonique; Committee of the International Telecommunication Union.
COBOL	COmmon Business-Oriented Language.
COS	Corporation for Open Systems.
CPU	Central Processing Unit.
DBMS	Data Base Management System.
DRAM	Dynamic Random Access Memory.
EIA	Electronic Industries Association.
EPROM	Erasable, Programmable, Read-Only Memory.
IEEE	Institute of Electrical and Electronics Engineers.
ISDN	Integrated Services Digital Networks.
ISO	International Organization for Standardization; voluntary international standards organization and member of CCITT.
ITU	International Telecommunication Union.

LSI	Large-Scale Integration.
MFJ	Modified Final Judgment.
PROM	Programmable, Read-Only Memory.
RBOC	Regional Bell Operating Company.
UNIX	AT&T Proprietary Operating System.
UPS	Uninterruptable Power Source.
VAR	Value-Added Reseller.
VLSI	Very Large Scale Integration.
WORM	Write-Once-Read-Many-Times.



Policies, Regulations, and Standards

A

OMB Circulars

A-11	Preparation and Submission of Budget Estimates.
A-49	Use of Management and Operating Contracts.
A-71	Responsibilities for the Administration and Management of Automatic Data Processing Activities.
A-109	Major Systems Acquisitions.
A-120	Guidelines for the Use of Consulting Services.
A-121	Cost Accounting, Cost Recovery, and Integrated Sharing of Data Processing Facilities.
A-123	Internal Control Systems.
A-127	Financial Management Systems.
A-130	Management of Federal Information Resources.
A-131	Value Engineering.

B

GSA Publications

The FIRMR as published by GSA is the primary regulation for use by federal agencies in the management, acquisition, and use of both ADP and telecommunications information resources.

C

DoD Directives

DD-5000.1	Major System Acquisitions.
DD-5000.2	Major System Acquisition Process.
DD-5000.11	DoD Data Elements and Data Codes Standardization Program.
DD-5000.31	Interim List of DoD-Approved, High-Order Languages.
DD-5000.35	Defense Acquisition Regulatory Systems.
DD-5200.1	DoD Information Security Program.
DD-5200.28	Security Requirements for Automatic Data Processing (ADP) Systems.

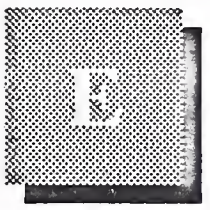
	DD-5200.28-M	Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems.
	DD-7920.2	Major Automated Information Systems Approval Process.
	DD-7935	Automated Data Systems (ADS) Documentation.

D

Standards

ADCCP	Advanced Data Communications Control Procedures; ANSI Standard X3.66 of 1979; also NIST FIPS 71.
CCITT G.711	International PCM standard.
CCITT T.0	International standard for classification of facsimile apparatus for document transmission over telephone-type circuits.
DEA-1	Proposed ISO standard for data encryption based on the NIST DES.
EIA RS-170	Monochrome video standard.
EIA RS-170A	Color video standard.
EIA RS-464	EIA PBX standards.
EIA RS-465	Standard for Group III facsimile.
EIA RS-466	Facsimile standard; procedures for document transmission in the General Switched Telephone Network.
EIA RS-232-C	EIA DCE to DTE interface standard using a 25-Pin connector; similar to CCITT V-24.
EIA RS-449	New EIA standard DTE to DCE interface which replaces RS-232-C.
FED-STD 1000	Proposed Federal Standard for adoption of the full OSI reference model.
FED-STD 1026	Federal Data Encryption Standard (DES) adopted in 1983; also FIPS 46.
FED-STD 1041	Equivalent to FIPS 100.
FED-STD 1061	Group II Facsimile Standard (1981).
FED-STD 1062	Federal standard for Group III facsimile; equivalent to EIA RS-465.
FED-STD 1063	Federal facsimile standard; equivalent to EIA RS-466.
FED-STDs 1005, 1005A-1008	Federal Standards for DCE Coding and Modulation.
FIPS 46	NIST Data Encryption Standard (DES).
FIPS 81	DES Modes of Operation.

FIPS 100	NIST Standard for packet-switched networks; subset of 1980 CCITT X.25.
FIPS 107	NIST Standard for local area networks, similar to IEEE 802.2 and 802.3.
FIPS 146	Government Open Systems Interconnection (OSI) Profile (GOSIP).
FIPS 151	NIST POSIX (Portable Operating System Interface for UNIX) standard.
IEEE 802.2	OSI-Compatible IEEE standard for data-link control in local area networks.
IEEE 802.3	Local area network standard similar to Ethernet.
IEEE 802.4	OSI-compatible standard for token-bus local area networks.
IEEE 802.5	Local area networks standard for token-ring networks.
IEEE P1003.1	POSIX standard, similar to FIPS 151.
MIL-STD-188-114C	Physical interface protocol similar to RS-232 and RS-449.
MIL-STD-1777	IP-Internet Protocol.
MIL-STD-1778	TCP - Transmission Control Protocol.
MIL-STD-1780	File Transfer Protocol.
MIL-STD-1781	Simple Mail Transfer Protocol (electronic mail).
MIL-STD-1782	TELNET - virtual terminal protocol.
MIL-STD-1815A	Ada Programming Language Standard.
SVID	UNIX System Interface Definition.
X12	ANSI standard for Electronic Data Interchange
X.21	CCITT Standard for interface between DTE and DCE for synchronous operation on public data networks.
X.25	CCITT standard for interface between DTE and DCE for terminals operating in the packet mode on public data networks.
X.75	CCITT standard for links that interface different packet networks.
X.400	ISO Application-level standard for the Electronic transfer of messages (electronic mail).



Related INPUT Reports

- *Federal Telecommunications Market, 1990-1995*
- *U.S. Industry Sector Markets, 1991-1996—Telecommunications Sector*
- *Procurement Analysis Reports, GFY 1991-1997*
- *Federal Systems Integration Market, 1990-1995*
- *Federal Professional Services Market, 1990-1995*
- *Federal Computer Equipment Market, 1991-1996*